NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A SURVEILLANCE SOCIETY AND THE CONFLICT STATE: LEVERAGING UBIQUITOUS SURVEILLANCE AND BIOMETRICS TECHNOLOGY TO IMPROVE HOMELAND SECURITY

by

Richard E. Makarski

and

Jose A. Marrero

September 2002

Thesis Advisor:	Alex Bordetsky
Associate Advisor:	Dale Courtney

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: A Surveillance Society and the Conflict State: Leveraging Ubiquitous Surveillance and Biometrics Technology to Improve Homeland Security			**5. FUNDING NUMBERS**
6. AUTHOR (S) Richard E. Makarski and Jose A. Marrero			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The thesis research examines the emergence of surveillance and biometrics technologies as a pragmatic baseline supporting the goals of homeland security. Assessment of existing catalysts of the world condition, conflict states, terrorist and criminal networks have facilitated increased U.S. and international attention to the field of surveillance and biometric technology. This study scrutinizes surveillance, biometric techniques, strategies, and prevailing present day applications. It contrasts the evolving requirements for improved security with a balanced consideration of civil liberties and privacy. The authors address developmental issues surrounding the hypothesis for a ubiquitous surveillance grid to monitor and combat terrorism, crime, and other contributing illicit behaviors. The authors recommend that federal, state, local, and corporate agencies unite in improving homeland security by implementing the deterrence, detection, monitoring, and response actions that these technologies have to offer.

14. SUBJECT TERMS Ubiquitous Computing, Surveillance, Biometrics, Homeland Security, Terrorism, Civil Liberties, Information Privacy			**15. NUMBER OF PAGES** 262
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A SURVEILLANCE SOCIETY AND THE CONFLICT STATE: LEVERAGING UBIQUITOUS SURVEILLANCE AND BIOMETRICS TECHNOLOGY TO IMPROVE HOMELAND SECURITY

Richard E. Makarski
Lieutenant Commander, United States Navy
B.S., Richard Stockton State College, 1989
M.B.A., Embry-Riddle Aeronautical University, 1993

Jose A. Marrero
Lieutenant, United States Naval Reserve
B.S., University of California, San Diego, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2002

Authors: Richard E. Makarski

Jose A. Marrero

Approved by: Alex Bordetsky, Thesis Advisor

Dale Courtney, Associate Advisor

Dan Boger, Chairman
Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The thesis research examines the emergence of surveillance and biometrics technologies as a pragmatic baseline supporting the goals of homeland security. Assessment of existing catalysts of the world condition, conflict states, terrorist and criminal networks have facilitated increased U.S. and international attention to the field of surveillance and biometric technology. This study scrutinizes surveillance, biometric techniques, strategies, and prevailing present day applications. It contrasts the evolving requirements for improved security with a balanced consideration of civil liberties and privacy. The authors address developmental issues surrounding the hypothesis for a ubiquitous surveillance grid to monitor and combat terrorism, crime, and other contributing illicit behaviors. The authors recommend that federal, state, local, and corporate agencies unite in improving homeland security by implementing the deterrence, detection, monitoring, and response actions that these technologies have to offer.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS, ACRONYMS AND SYMBOLS

1:1:	One-to-One, within subject variability
1:N:	One-to-Many, between subject variability
3D:	Three-dimensional
9-11:	11 September 2001 (Date of worst terrorist attack in U.S. history)
ACE:	Automated Customs Environment
ACI:	Ancore Cargo Inspector
ACLU:	American Civil Liberties Union
ACS:	Automated Customs System
AES:	Advanced Encryption Standard
AFIS:	Automated Fingerprint Identification System
AFL-CIO:	American Federation of Labor-Congress of Industrial Organizations
AIDS:	Acquired Immune Deficiency Syndrome
ANSI:	American National Standards Institute
APHIS:	Animal, Plant, and Health Inspection Service
ATM:	Automated Teller Machine
CABS:	Computerized Arrest and Booking System
CAC:	Common Access Card
CBRN:	Chemical, Biological, Radiological, and Nuclear
CCTV:	Closed Circuit Television
CDC:	Centers for Disease Control
CEO:	Chief Executive Officer
CERT:	Community Emergency Response Teams
CHEMBIO:	Chemical Biological
CIA:	Central Intelligence Agency
CIO:	Chief Information Officer
CIP:	Critical Infrastructure Protection
CNN:	Cable News Network
CSG:	Counterterrorism Security Group

CSS:	Cybercorps Scholarship for Service
CTIT:	Counter-Terror Information Technology
CWIN:	Cyberspace Warning Intelligence Network
DARPA:	Defense Advanced Research Projects Agency
DCS:	Distributed Control System
DEA:	Drug Enforcement Agency
DMV:	Division of Motor Vehicles
DOA:	Department of Agriculture
DOD:	Department of Defense
DOE:	Department of Energy
DOJ:	Department of Justice
EDS:	Explosive Detection System
EER:	Equal Error Rate
EPIC:	El Paso Intelligence Center
ERF:	Emergency Response Fund
ETD:	Explosive Trace Detector
EU:	European Union
EUROJUST:	European Judicial Cooperation Unit
FAA:	Federal Aviation Administration
FAR:	False Accept Rate
FBI:	Federal Bureau of Investigation
FBI:	Federal Bureau of Investigation
FEMA:	Federal Emergency Management Agency
FinCEN:	Financial Crimes Enforcement Network
FLIR:	Forward Looking Infrared
FRR:	False Rejection Rate
FTC:	Federal Trade Commission
FY:	Fiscal Year
GAO:	General Accounting Office
GovNet:	Government Network

GPS:	Global Positio ning System
GSA:	General Services Administration
HAN:	Health Alert Network
HHS:	Health and Human Services
HIV:	Human Immunodeficiency Virus
HLS:	Homeland Security or Homeland Security Department
HR:	House Resolution
ID:	Identification
INPASS:	Immigration and Naturalization Passenger Accelerated Service System
INS:	Immigration and Naturalization Service
IRS:	Internal Revenue Service
IT:	Information Technology
LFMI:	Low Frequency Magnetic Imaging
MAV:	Micro Air Vehicle
MEMS:	Micro Electro-Mechanical Systems
NCIS:	National Crime Information System
NDP:	National Defense Panel
NIH:	National Institutes of Health
NIPC:	National Infrastructure Protection Center
NISAC:	National Infrastructure Simulation and Analysis Center
NIST:	National Institute of Standards and Technology
NSA:	National Security Agency (or National Security Adviser)
PARC:	Palo Alto Research Center
PC:	Personal Computer
PDA:	Personal Digital Assistant
PDB:	Presidential Daily Brief
PFNA:	Pulsed Fast Neutron Analysis
PIN:	Personal Identification Number
PWA:	Priority Wireless Access
QDR:	Quadrennial Defense Review

RFP:	Request for Proposal
RODS:	Real-Time Outbreak and Disease Surveillance
SCADA:	Supervisor Control and Data Acquisition
SIPRNET:	Secret Internet Protocol Router Network
SPIdS:	Secure Perimeter Identification System
SR:	Senate Resolution
SSA:	Social Security Administration
SSN:	Social Security Number
TES:	Time Encoded Speech
TESPAR:	Time Encoded Signal Processing and Recognition
TIPS:	Terrorist Information and Prevention System
TNA:	Thermal Neutron Analysis
TSA:	Transportation Security Administration
TSA:	Transportation Security Agency
TTP:	Trusted Third Party
UAV:	Unmanned Aerial Vehicle
UCAV:	Unmanned Combat Aerial Vehicles
UK:	United Kingdom
USAMRIID:	U.S. Army Medical Research Institute of Infectious Diseases
USCS:	United States Customs Service
USDA:	United States Department of Agriculture
V-EDS:	Vehicular Explosive Detection System
VIPS:	Volunteers in Police Service
WHO:	World Health Organization
WMD:	Weapons of Mass Destruction
WTC:	World Trade Center
XML:	Extensible Markup Language

ACKNOWLEDGMENTS

We would like to acknowledge and thank the following people and organizations:

To our wives, Kaye Makarski and Linda Marrero, for their unwavering support during our academic emersion at the Naval Postgraduate School. The thousands of hours of reading, writing, study and research during our 27-month experience was made easier by their love and understanding. We could not have done it without you.

To our Thesis Advisor Professor Alex Bordetsky, for his enthusiasm and support for the field of ubiquitous computing and surveillance.

To our Associate Thesis Advisor Dale Courtney, for his methodical and comprehensive reviews from proposal to final chapter. His guidance and analytical appraisal throughout the entire thesis effort helped make this broad area of study a more digestible and intriguing learning experience.

To Professor Frank Barrett, for his insight to managing change in complex organizations. Thank you for enabling us to appreciate the broader system's view of the world and better understand the complexities of people and their role with technology and processes.

To the staff of the Dudley Knox Library for their tremendous support in providing quality study environments, research assistance, and literature resources to complete our thesis work and all our related academic assignments.

To the staff at the ANSER Institute for Homeland Security for the literature resources provided through their highly organized web site. Their thoughtful consolidation of homeland security related news, articles, white papers, research, and publications reflect their vision for being change agents and catalysts for innovative thinking. Their leadership in the field of homeland security serves as a first-class example for collaboration building and improving public awareness and education.

To all the staff at the Naval Postgraduate School, thank you for the honor and privilege to attend this prestigious and historic institution. The quality education we have received has better prepared us for the challenges that lie ahead in service to our country and sharpened our critical thinking skills for leadership roles we will command.

Finally, to all those too numerous to mention, who serve as guardians working for a better world, we give thanks. To the first responders in the medical, firefighting, rescue, and law enforcement communities, thank you for your work. To the uniformed services, intelligence communities, researchers, scientists, scholars, and legislators, thank you for your work. The world is an imperfect and fragile place; the unity we are experiencing as a nation and international community in combating terrorism and crime is the inspiration that will carry us to a more secure future.

I. INTRODUCTION

A. PURPOSE

This thesis focuses on the examination of available and emerging surveillance and biometric technologies for the purpose of improving homeland security, national defense, and creating a safer world. It will reveal the broad spectrum of potential methods that may be used in the deterrence, detection, monitoring, and response actions against terrorism, crime, and other illicit behavior. The technical, cultural, and legal issues of using surveillance and biometric technology within society will be exposed and addressed to provide balance to this challenging discussion. The authors of this research contend that the key to a safer world lies in embracing this technology and the willingness for humanity to adapt to change.

B. MOTIVATION

The terrorist attacks against America on September 11th 2001 (9-11) killed more Americans (over 3,000 dead) than the Japanese attack on Pearl Harbor on 7 December 1941 (2403 dead) and brought us intimately closer to the realization that the unthinkable was now possible on our home soil—that civilians are not immune from becoming the brunt of conflict casualties. The 9-11 attack on American marked a sober turning point in the way we live our lives, conduct business, operate public transportation, and employ law enforcement strategy and tactics. It emphasizes the need for the United States and all civilized nations to collaborate and make ready the innovative and dramatic efforts by which we can prevent acts of violence and crimes against humanity. As we witness societal changes, religious indifferences, cultural clashes, and the instability caused by erosion of standards and values, we must brace ourselves for more conflicts and prepare appropriate measures for managing the consequences of human misbehavior. Human beings typically enjoy their privacy, yet as we hear the news reported daily from domestic and international sources—terrorism, crime, and brutal acts of hatred have civilized peoples asking questions on how we can protect ourselves. This thesis is not the complete answer to the dilemma that we face today in detecting terrorist activity and

crime, but it plants the seeds of progress for which technology and innovative minds can devise effective solutions in leading us into a more secure future.

C. RESEARCH QUESTIONS

The primary research question addressed in this thesis is: Can ubiquitous surveillance and biometric technologies provide the layered solutions to defend against terrorism, crime, and other illicit behaviors?

Secondary research questions include the following:

- Why have we arrived at this crossroad in society? What are the historical catalysts that have brought us to seek surveillance and biometric technology as resources to manage conflict and world instability?
- What is the national strategy for homeland security that provides basis for employment of such technology?
- How does this technology work? To what applications has this technology already been applied? In what ways can it be deployed in the future?
- Of the many biometric methods of surveillance, authentication, and detection—which seem to be the most promising in the near term?
- What are the probable impacts of ubiquitous surveillance on society?
- What are some of the critical success factors, which must be considered to implement ubiquitous surveillance from the concept stage to real world usability?

D. SCOPE OF THESIS

This thesis will encompass the present array of surveillance and biometric technologies; it will discuss areas of possible deployment and reveal its benefits to society as well as its present shortcomings, including technical and legal issues. Furthermore, it will suggest possible implementation strategies based on lessons-learned from past and present initiatives. Special attention will be given to the United Kingdom, which notably has the greatest experience in this field and which at present has the largest concentration of surveillance infrastructure in the world. The ultimate goal of this thesis is to suggest intelligent uses and strategies for using surveillance and biometric technology to improve homeland security. The resulting recommendations are intended to provide a more effective concept model for defending against crime and terrorism for the future of civilization.

E. METHODOLOGY

The methodology used in this thesis research will consist of the following steps:

- Conducting a literature review of Internet sources, newspapers, magazine articles, books, and other information sources for material relevant to the study of surveillance and biometrics and the catalysts prompting the use of this technology.
- Carrying out a review of present and evolving surveillance and biometrics initiatives, legislation, policies, and societal issues.
- Collecting and analyzing reviews of various surveillance and biometric devices.
- Aligning surveillance and biometric applications to the strategic goals of homeland security.
- Developing a suggested concept for employing ubiquitous surveillance and biometrics in society.

F. ORGANIZATION OF STUDY

- Chapter II discusses the catalysts for surveillance and biometric technology in society. It discusses the escalating conflict state, which has brought us to the culminating point in the war on terrorism. It examines components of human activity and addresses specific areas of opportunity where surveillance and biometrics can have practical impact in crime prevention, security, and public safety.
- Chapter III provides the reader with the background on the creation of the evolving Department of Homeland Security. It discusses the organization, strategies, and objectives of homeland security as well as the role technology will play in shaping a safer world.
- Chapter IV examines the classes of existing and emerging surveillance and biometrics technologies and compares the various capabilities.
- Chapter V discusses the various existing and proposed applications of specific surveillance and biometrics technology.
- Chapter VI provides an insight into the impacts and ethics of surveillance and biometric technology upon society. It also provides an overview of current and emerging legislation and policies, which aim to balance the need for more effective protection against crime and terrorism while addressing the maintenance of civil liberties and personal privacy.
- Chapter VII provides a conclusion, critical success factors, and recommendations based on best available information. The concept for ubiquitous surveillance and biometrics is presented not as an instant cure for terrorism, crime, and societal dysfunction, but as an evolving and

layered approach to managing the friction, conflicts, and hazards in the new global environment in which we live, work, and play.

II. THE CATALYST FOR UBIQUITOUS SURVEILLANCE

A. WHY WE ARE AT THIS CROSSROAD

Why is surveillance capturing so much of the current headlines, and why is technology primed for responding?

Although there are numerous specific reasons that can be attributed as catalysts for a surveillance society, this chapter will broadly discuss two major themes that attempt to examine why we are at this crossroad. First is world conflict. Managing economic, environmental, political, and social change in a world that is growing rapidly in population yet is dwindling in resources, produces increased potential for a wide range of conflicts. Second, sophistication in computer and information technologies have reached such a level of maturity that modern societies feel compelled to utilize these resources to more efficiently monitor, sense, detect, and manage human activity for the greater good of a peaceful civilization.

Expanding on the first catalyst, the world is becoming a more fragile and ever volatile place to live. Scarcity of resources, overpopulation, crime, tribalism, ethnic discourse, religious fanaticism, and disease are producing waves of instability throughout the globe. Managing this global trend is complex because of the numerous political, military, environmental, and socio-cultural variables. There is now a blurring of separation between wars among nation states and organized criminal organizations, and the large-scale violations of human rights against the innocent (World Global Trends, 2002). Where there is disparity and inequity, conflicts, civil strife, and victimization abound. The global trends and statistics are alarming.

> "In the next hour, global population will increase by 8,300 people; in 24 hours, there will be an additional 200,000 mouths to feed; as many as 73 million people are being added to our planet every year, while resources available to feed them are diminishing." (Future Harvest, 8 May 2002).
>
> "If current trends continue, 2.7 billion people will not have enough water by 2025. Approximately 800 million people go hungry every day, 95 percent of them reside in the developing countries." (Future Harvest, 8 May 2002).
>
> "To keep pace with current population growth, world subsistence resources must increase 50 percent by the year 2020." (Future Harvest, 8 May 2002).

"More than 40 percent of the world's fish stocks have been fished to their biological limit." (Future Harvest, 8 May 2002).

"Presently, more than 1.3 billion people in developing countries live in abject poverty, surviving on incomes of less than one dollar a day, while another 2 billion people are only marginally better off." (Future Harvest, 8 May 2002).

"The poor of the world seldom have enough for a nourishing diet, education, family planning, or medical care; women and children are typically the most vulnerable." (Future Harvest, 8 May 2002).

"Over the last 20 years, violent conflicts have killed an estimated 20 million people worldwide—90 percent of the victims have been non-combatants, mostly women and children." (Future Harvest, 8 May 2002).

"By the mid-1990s, the annual costs of international peacekeeping and emergency humanitarian assistance due to wars reached 10 billion dollars." (Future Harvest, 8 May 2002).

"War often destroys food crops, leaving people without a source of food or income and laying the groundwork for continued conflict. In the past decade, armed conflict has killed more than 2 million children and has maimed another 6 million children." (Future Harvest, 8 May 2002).

"Each year, approximately 26,000 civilians are killed or maimed by landmines." (Future Harvest, 8 May 2002).

"The human immunodeficiency virus (HIV), which causes AIDS, has brought about a global epidemic far more extensive than what was predicted even a decade ago. Unless a large-scale anti-HIV/AIDS campaign is launched, experts fear 50 million people will be infected with HIV by 2005." (World Global Trends, 2002).

"World oil production will begin declining by 2010. The result will be higher energy prices and global economic disturbances, according to Princeton University geologist Kenneth S. Deffeyes." (World Future Society, 2002).

"The twentieth century has seen over 250 wars, including two world wars and a cold war, with more dead than in all previous wars over the past two millennia." (World Global Trends, 2002).

"Weapons proliferation experts project that at least 20 to 25 countries have developed or may be currently developing nuclear, biological, or chemical weapons; and that poorer and less technologically advanced countries may be seeking chemical and biological weapons." (World Global Trends, 2002).

Exacerbating the previously mentioned trends is the growth of international terrorism and crime organizations. These factors contribute to increasing world conflict and instability, which further elevate concerns for public safety, protection of critical

infrastructure, weapons proliferation, and eroding natural resources. These issues have become major concerns on the American public stage, but none more so than the current headline – "terrorism."

The Hart-Rudman Commission concluded in its final report that the United States will face a terrorist attack by an adversary within the next 20-30 years that will cause thousands of American causalities (Roxborough, Sep 2001). The issues surrounding the Hart-Rudman Commission study revolve around world change and the impact of globalization on society. Globalization has brought hope for the future prosperity of an integrated society, and along with it, a certainty of conflicts as a number of cultures reject concepts of modernity. Globalization has produced byproducts of unpredictability and vulnerability. It has increased our interdependence with world nations, yet simultaneously it has created more conflict, not less (World Global Trends, 2002). The global separation between the societies that benefit in the coming era and those that flounder in the suffrage of economic and social inequity will likely create further conditions of instability that will trend toward regional or international conflicts. This is not to imply that all changes brought on by globalization are bad for society, nor does it suggest that we avoid change in order to secure world stability. It does put forth a cautionary footnote however, for the strong linkage between terrorism and the growing divide between struggling nations and the nations that prosper. The threats to the civilized world have become all too real. The implied obligation for the world superpowers to find a solution has never been greater. Speculating on threat assessment and what specifically might cause the next conflict for America and other peace-loving nations can quickly become a philosophical debate with no end. Yet if we use history as a benchmark—for example, terrorism during the last ten years—we tempt to predict the future U.S. threats and take an academic position based on empirical analysis. This analysis can logically conclude that short and long-term threats from foreign and domestic sources are inevitable and unavoidable. Global conflicts in general are on the rise, as is the accessibility of weapons of mass destruction. As of 1 January 2001, the world was still grappling with a hodgepodge of problems left over from the 20th century. There are still more than three-dozen major active conflicts in the world (Figure 2.1) in

which over 1,000 or more casualties have been reported (Smith, 1 Jan 2001). World conflict and terrorism are increasing in spite of our best efforts.

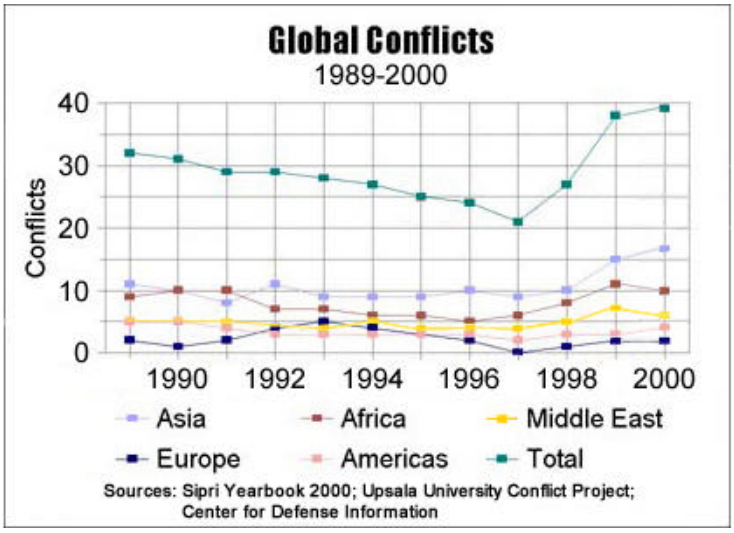


Figure 2.1. Global Conflicts 1989-2000. (From: Smith, 1 Jan 2001).

Terrorism, as it relates to global conflict, is also on the rise. International terrorist attacks have shown to be increasing in scale and lethality. The number of dead and wounded in terrorist attacks is on the rise as international terrorist organizations acquire more sophisticated methods of assault. In 2000, 409 persons died in terrorist attacks while 796 were wounded. In 2001, a total of 3,547 persons were killed in terrorist attacks while 1,080 were wounded (U.S. Department of State, May 2002). Although the gross number of actual attacks has dropped from previous years to 348 in 2001, from 426 in 2000 (Figure 2.2 and Figure 2.3), the trend is toward better-planned terrorist events that result in additional human carnage and greater perceived impact toward the terrorists' cause. In addition to the horrific casualties inflicted upon the United States in the September 11th 2001 terrorist attacks, violence in the Middle East and South Asia also accounted for the increase in casualty totals for 2001 (Figure 2.4, U.S. Department of State, May 2002). Israeli-Palestinian violence significantly escalated in 2001, resulting in almost 200 Israelis and over 500 Palestinians killed (U.S. Department of State, May 2002).

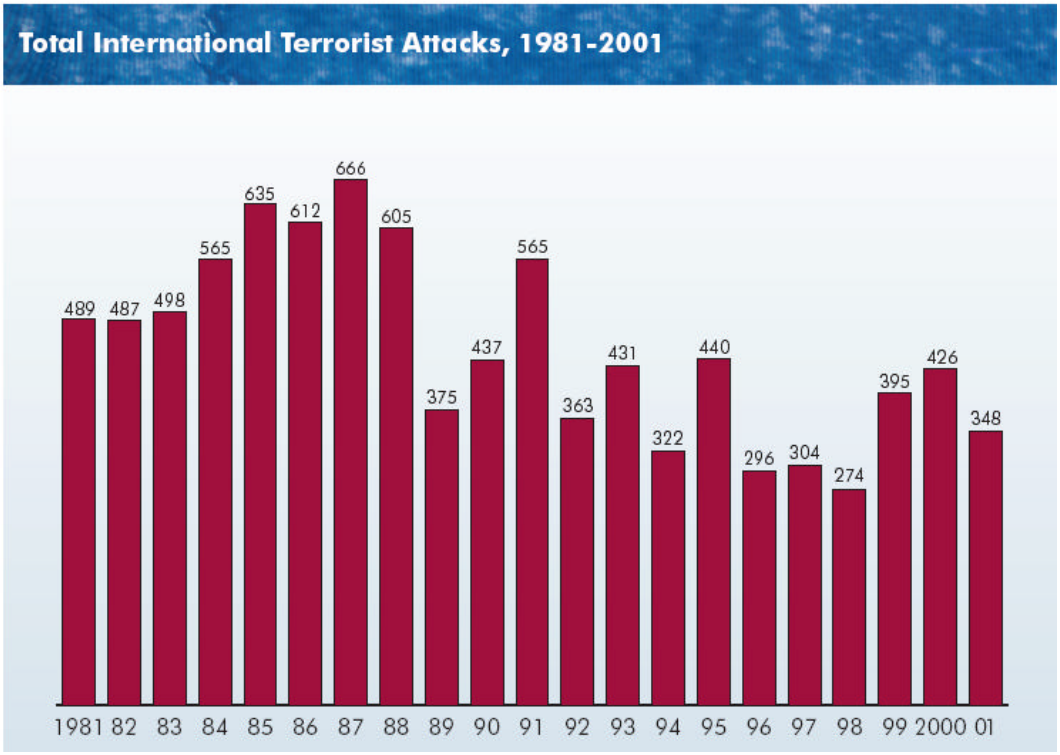


Figure 2.2. Patterns of Global Terrorism, Attacks 1981-2001. (From: U.S. Department of State, May 2002).

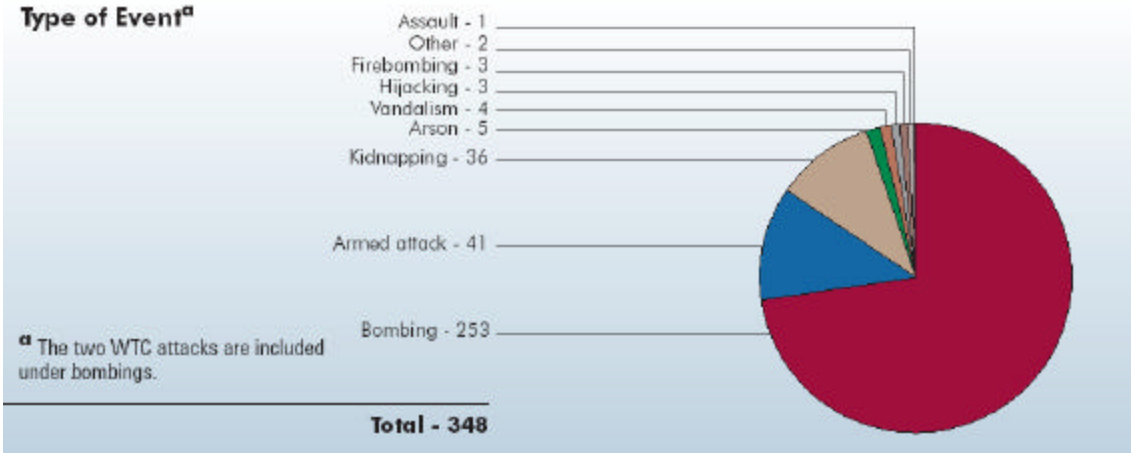


Figure 2.3. Patterns of Global Terrorism, Type of Event 2001. (From: U.S. Department of State, May 2002).

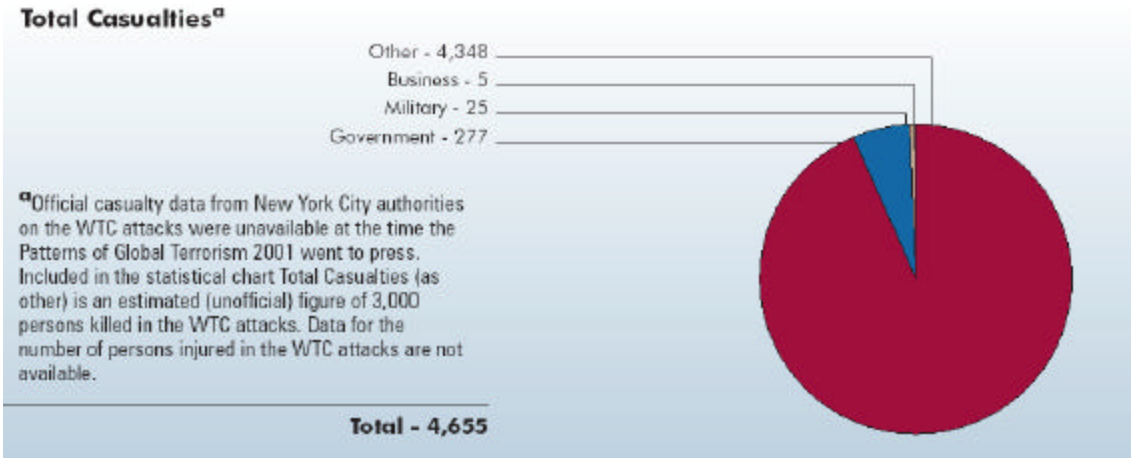


Figure 2.4. Patterns of Global Terrorism, Total Casualties 2001. (From: U.S. Department of State, May 2002).

Violence against America has previously shown to originate from state sponsored groups, non-state sponsored groups, individuals, and hybrids of these. As we go forth, we need to be vigilant of aggression from all sides, yet not submit to paralysis, which can overtake caution. The real danger that exists now is that U.S. policymakers may view any change as leading to instability, and therefore succumb to a stagnation effect, which would be counterproductive to improving global economic and social prosperity for all. Doing nothing is not an option. America must have focus and build global coalition to manage the changes that lie ahead.

Analysts predict that over the next 25 years, foreign crises will continue to be replete with atrocities and the deliberate terrorizing of civilian populations. Numerous cross-border wars are forecast with the most violence erupting from conflicts internal to current territorial states (World Global Trends, 2002). As many governments fail to adapt and modernize to the new economic and social realities, people's desires for independence will proliferate, and minorities will be less likely to accept injurious government practices. As a direct result of this friction, international conflict and violence will be exacerbated, springing newly created zones of autonomy, leaving major powers to struggle in developing effective institutional responses to such crises (World Global Trends, 2002). If one can grasp in this research the appreciation for current global

fragility, you begin to understand that the stage is now being set for a new world where monitoring and sensing have become consequential yet necessary requisites for survival.

It may be suggested that the intelligent U.S. approach to managing change in this complex world is to face the inevitable spheres of instability with a thoughtful strategy that adapts to the forces of global transformations that it cannot expect to have total control (Roxborough, Sep 2001). Ubiquitous surveillance holds promise for just such a strategy, for if you cannot control the actions of others, you can at least monitor them and be prepared to respond with intelligent and deliberate countermeasures.

The second reason we are at this crossroad is because our position in technology has matured to such a state that we are now poised at the eve of the third wave of computing – "ubiquitous computing" or "calm computing." The first wave in computing technology was mainframe computing, one processor serving many people. The second wave in computing was dubbed "Personal Computing" or PC computing, one processor serving one person. Now we enter into this third, most enveloping wave, called ubiquitous computing, many processors serving each person (Xerox PARC, 2001). Hence, the idea of "ubiquitous surveillance" comes from this broader concept of ubiquitous computing—a term coined by the "Father of Ubiquitous Computing," Dr Mark Weiser (Xerox PARC, 2001). The term "ubiquitous" means being or seeming to be everywhere at the same time. Dr. Weiser proposes that the most powerful technologies are those that disappear into the background of daily living; they weave themselves into the fabric of everyday life until they are indistinguishable from it (Xerox PARC, 2001). The miniaturization of computing and the subsequent surge in processing efficiencies have transitioned humankind to a new era. Surveillance and sensing technologies thus begin to be transparent around us, becoming smaller and more powerful at processing tasks. Therefore, ubiquitous surveillance will become omnipresent. In the future, surveillance will become so pervasive and efficient that we will cease to be aware we are being watched, screened, observed, and protected. The key to success in the ubiquitous surveillance concept model is that the technology is complementary to our lives and unobtrusive to human daily activity. The new world unfolding before us in the decades ahead is predicted to be a place in which we will co-exist harmoniously in sensor-rich

environments. Small ubiquitous computing devices will monitor everything from who is knocking at your door, to where your child is at any moment in time, to what is inside that cargo shipping container transiting the ocean (Xerox PARC, 2001). In the not too distant future, analysts predict that you will not need a password or PIN because in fact you will be the password or PIN (Rolwing, p. 11). In biometric terms, a computing sensor will validate who you are based on your biological signature. Your eyes, face, fingerprint, hand, or voice, will authenticate your identity. The concept of biometrics is built upon the theory that authentication of who you are is a measurable and verifiable science. One's own biological signature of uniqueness is distinguishable and quantifiable using sensor-based technologies. The technologies can be used toward numerous applications where security, safety, and personal identification are necessary requirements. The increasing accuracy of biometrics technology has evolved to provide a natural partnership with surveillance technology, especially for the surveillance of human behavior.

The need for ubiquitous surveillance has grown not of voyeuristic motives but one of securing public safety, prevention, detection of criminal activity, counter-terrorism, protection of national assets, and intelligence gathering for national defense. Ubiquitous surveillance can alert authorities to take corrective actions to right a wrong, capture a perpetrator, intercept a disaster in the making, and save lives.

Several credible polls suggest a majority of Americans welcome surveillance in society for their own protection, and there is growing public support for broadening the government's investigative powers for defense purposes (Thorsberg, 8 Oct 2001).

A Harris Poll performed 19-24 Sep 2001, surveyed 1,012 adults and found that,

- 86 percent support face-recognition technology to scan for suspected terrorists at various locations and events;
- 81 percent wanted closer monitoring of banking and credit card transactions, and 68 percent favored a national identification system, and;
- More than half of the respondents supported government monitoring of Internet discussions and chat rooms and increased monitoring of mobile communications and e-mail (Thorsberg, 8 Oct 2001).

In a BusinessWeek poll held in October 2001,

- More than 60 percent of 1,334 respondents said a national ID card system was acceptable and that they would submit to a facial scanning system in connection with transit or large public events;
- Slightly more than 50 percent expressing support for expanded scanning of email messages and phone conversations by the government; and
- Nearly 50 percent supported additional wiretapping and email surveillance (Thorsberg, 8 Oct 2001).

B. TERRORISM

The morning of September 11, 2001 unfolded the worst act of terrorism in U.S. history and was without a doubt, the greatest awakening Americans have ever had that such deadly violence can be a domestic reality. Osama bin Laden, Mohamed Atta, and the terrorist network "al Qaeda" are now names known throughout the world. Prior to this horrific event, the last decade has been filled with major terrorist incidents that have given clue to impending dangers to come. Here is a short chronology (Davis, Jan 2002):

- On 26 Feb 1993, a car bomb in the World Trade Center killed six, injured 1000, and caused over $600 million in damage;
- On 20 Mar 1995, a Japanese extremist group launched a coordinated attack within the Tokyo subway system by releasing the nerve agent sarin on commuter trains at rush hour, killing 12 people and injured over 5,500 others;
- On 19 Apr 1995, a truck bomb exploded outside the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, killing 168 people, and injured hundreds;
- On 25 Jun 1996, terrorists attacked a U.S. military barracks, the Al Khobar Towers in Saudi Arabia, killing 19 airmen;
- On 7 Aug 1998, terrorists bombed the U.S. Embassies in Tanzania and Kenya, killing 224, including 12 Americans;
- In May 2000, the "I Love You" computer virus attack caused over $15 billion in damage to United States commercial and government agencies, and infected and forced off-line 70% of the computers in Scandinavia and Germany;
- On 12 Oct 2000, a suicide bomber attacked the USS Cole while in the port of Aden, Yemen, killing 17 American sailors and injuring 39 others;
- And finally, in the worst case of terrorism on U.S. soil, on 11 September 2001, 19 terrorist hijacked four airliners, crashing them into the World

> Trade Center twin towers, the Pentagon, and a field in Stony Creek Township, Pennsylvania, killing over 3,000 people and injuring hundreds (Davis, Jan 2002).

Since 1968, there have been more than 10,000 recorded incidents of terrorism worldwide, yet until recently, the resulting fatality rates experienced have been anywhere from one, to just under 100 per event (Hoge and Rose, pp. 4-5). Although the earlier causes of terrorism are believed to be entrenched in poverty and inferior living conditions, we are also seeing a more sinister terrorist movement evolving, spurred by religious ideology (World Future Society, 2002). These modern terrorist factions have fewer moral qualms about mass murder, and still fewer concerns about what their constituents might think of their perpetrating murder on an even greater scale (Hoge and Rose, p. 5). These religiously inspired terrorists welcome their own death with as much enthusiasm as they have in carrying out the deaths of their intended victims. They murder with the belief that God's cause will bring them rewards in the afterlife (Hoge and Rose, p. 5). Because of this view, suicide has become the quintessential benchmark of religious devotion among terrorist "true believers" in the Middle East (Hoge and Rose, p. 7). The Director of the FBI has stated unequivocally that it is inevitable the United States would one day see pedestrian suicide bombers on home soil and that terrorist attacks against the United States is a reality we will all have to face (CNN, 20 May 2002). What is most disconcerting is the possibility that weapons of mass destruction may get into the hands of terrorist organizations that would not hesitate to use them against civilian populations, potentially causing casualties in the tens of thousands or millions. Experts believe terrorists may also resort to the use of dirty bombs, which can be used along with conventional explosives to spread contaminating nuclear material over a large area (Haddock, 28 Apr 2002). Such a weapon could cause mass disruption and hysteria in a region or entire nation. It is now common knowledge that the question is not if, terrorist will attack again, but when, and how.

For years we have written off terrorism as something that largely happens overseas, that American soil was somehow immune from the reach of international religious fanaticism. Although Israelis have lived with suicide terrorism for many years, the reality is something most Americans are not prepared accept. The painful lessons of

9-11 have now propelled us to imagine the unimaginable. The news reels of passenger planes crashing into the World Trade Center, the Pentagon burning, and the subsequent bioterrorist attacks of anthrax-laden mail (Sep-Oct 2001) send a cold realism into the American psyche, that we are vulnerable and must fight back vehemently to preserve our freedom and the freedoms of all civilized people.

Ironically, it is partly because of the freedoms we cherish and openness we enjoy as an American society that we are so susceptible to terrorism. Historically, we have associated violence against America as a remote possibility but not one that we viewed as a mortal threat to thousands of innocent non-combatants in a single terrorist act. Before 9-11, Americans have stereotypically been more concerned with the U.S. economy and employment rather than domestic security and safety. Using airport security as an example our existing layers of security were mere window-dressing to make a flying public feel good about the appearance of airport security. We now know that the privately run airport security system was a product of the lowest bidder; sound training and substantive security measures were simply not thought of as an economic investment worth making (Fish, 2002). One GAO report revealed that the annual job turnover among airport screeners averaged 126 percent at the country's 19 largest airports with five airports having a rate significantly higher: Saint Louis (416%), Atlanta (375%), Houston (237%), Boston (207%), and Chicago (200%) (Fish, 2002).

The technological ability for terrorists to launch vicious attacks against civilian populations and critical infrastructure is spreading to larger numbers of terrorist organizations and individuals with each passing year. The threat of terrorism is an inescapable reality and permanent condition of life in the 21st century (Whitehouse, 2002). America must never relax its resolve to defeat terrorist wherever they live. Our Secretary of Defense, Donald Rumsfeld, said of terrorism plainly:

> It would seem to me that if one thinks about it, a terrorist can attack at any time at any place, using any conceivable technique. You and I know it's impossible to defend in every single location at every moment of the day or night against every conceivable type of technique. It can't be done. That means that the only way you can deal with terrorists is to go after them. The only defense against terrorism is offense. It is preemption. It

is finding them and rooting them out and stopping them. And it's dealing with the countries that harbor them. (Rumsfeld, 20 Feb 2002).

C. THE IMPERFECT FENCES AND WORLD VULNERABILITIES

One of the greatest assets of a terrorist is to remain anonymous, faceless, and nameless while exercising global mobility.

As the expansion of the Internet has made much of our personal and business lives easier, so too has it made the increased growth of identity theft and document fraud all the more dramatic. It has become apparent that identity theft is becoming one of the major stepping-stones for international crime groups, fraud rings, drug cartels, and terrorist organizations to accomplish their broader objectives.

Security vulnerabilities in our airports, seaports, border-crossings, and other hubs of transportation and commerce are being used to gain illegal access to physical locations, such as airplanes, federal buildings, computer systems, and other restricted areas. The potential damage that can be caused by terrorist organizations is so great that we can no longer afford to be reactive to the problems of personnel authentication and international security. The international community needs to be proactive in pursuing all possible solutions and preemptive measures, both technological and procedural, in addressing the points of weakness in our systems.

1. Borders and Ports

Our borders are typically the first physical lines of defense against terrorist infiltration to the U.S., but managing comprehensive control over such an extremely large area with the existing volume of traffic is an immense challenge. The U.S. shares a 7,500-mile border with Canada and Mexico along with an exclusive economic zone encompassing 3.4 million square miles (Whitehouse, 2002). Combine this with the fact that more than 500 million people enter into the United States each year, 67 percent (330 million) of which are non-citizens, one begins to get the magnitude of the border control challenge.

On the cargo side of commerce, over 11.2 million trucks and 2.2 million rail cars cross into the United States annually (Whitehouse, 2002). Our seaports are another access point to our borders, and no less high in traffic. By sea, 8,000 foreign-flag ships

with multinational crews make 51,000 calls in U.S. ports annually (Loy and Ross, Feb 2002). It would surprise most people to know that more than 95 percent of our non-North American foreign trade arrives by ship; and of the 7.5 million ship containers that enter the U.S. each year, only 2 percent are physically inspected for illegal or otherwise unauthorized materials or goods (Loy and Ross, Feb 2002). The rules that govern the inspection of commerce were never created with the thought that shipments might carry containers that could contain weapons of mass destruction (WMD), and it is economically self-defeating to attempt to inspect all contents of every shipment. Stoppages or slowdowns for freight inspections would have grave economic consequences globally since the world is dependent on commerce for goods from oil to food and every imaginable item in between.

In the air, U.S. and foreign airlines hauled 8.4 million freight tons to and from the United States during the year ended March 2001, a 3.6% increase from the previous year (USDOT, Mar 2001). U.S. and foreign air carriers also transported 144 million passengers between the United States and the rest of the world for the year-ending March 2001 (USDOT, Mar 2001). This represents a traffic increase of 7% over the previous year. As international commerce continues to grow, so does the concern that someday again, either by air, sea, or land, terrorists will use the weakest seams of our vulnerabilities to deliver a destructive blow to the civilized world.

2. Identification Theft

The anonymity of terrorists and the success of their operations can depend greatly on their ability to obtain false identification. According to the FBI, every two minutes someone is having their identity stolen; this equates to roughly 350,000 times per year and is increasing annually (Regan and Willox, 2 Oct 2001). The Federal Trade Commission (FTC), which maintains an Identity Theft Hotline and Identity Theft Data Clearinghouse, has seen a dramatic rise in reported identity theft, noting it received an average of over 1,800 reports per week in 2001 compared to 445 per week when the hotline started in November 1999 (Regan and Willox, 2 Oct 2001). The fraudulent use of social security numbers as reported by the Social Security Administration (SSA) has risen by 500% in just four years (Regan and Willox, 2 Oct 2001). Estimates of the number of

people victimized by identity theft in 2000 range from 500,000 to 700,000, and were approximately 750,000 in 2001. The Wall Street Journal estimates that identity theft cost consumers and merchants combined an estimated $1 billion in the year 2000 (Regan and Willox, 2 Oct 2001).

Since the terrorist attacks of September 11th, it has become know that some of the identities used by the hijackers in carrying out the terrorist plot were fraudulently obtained—false identities stolen from real people. It appears that the hijackers maintained their claimed identities with the use of phony passports, drivers' licenses, and other documents. The identities they used were of real people who live in Saudi Arabia and Tunisia.

Stolen passports previously issued to law abiding citizens can easily be altered to suit the terrorist's needs, and legitimate blank passports can be stolen to create authentic looking passports for similar purposes. Some of the 9-11 hijackers were able to forge Belgian passports. Furthermore, Belgian authorities have estimated that some 19,050 blank Belgian passports have gone missing or been stolen since 1990 (BBC, 21 Aug 2001). Organized international terrorists tend to assume identities of people in their native countries, or of that immediate area. Regrettably, most of the authentication resources and capabilities that exist today consist of only domestic or local information. Without having overseas information on foreign nationals, comprehensive checking on a global scale remains unrealistic (Regan and Willox, 2 Oct 2001).

Much has been stated concerning the potential benefit of using some form of biometrics in confirming identification of the international identity thief. It should be emphasized that both surveillance and biometrics techniques are only as good as the data available to authenticate the individual in question. For example, a computerized face recognition system designed to alert to the presence of a terrorist can only be useful if the individual's face is in the computer database (Regan and Willox, 2 Oct 2001). In the case where the database is normally populated with those who are known felons, then the system would not be able to detect a thief who is not yet known to be a criminal. However, when a system is supplemented by the corroboration of another piece of unique information such as a social security number or passport, then the system effectiveness

can be increased by an order of magnitude. When perpetrated by a professional criminal, identity theft is used as a means to cover up or conceal a much larger crime, which is why tracking identity theft is difficult and challenging work, especially as it relates to the world of terrorism. It is no surprise that the growth of the Internet has given this type of theft global reach, and quickly created greater tribulation for consumers, merchants, law enforcement, and policy makers (Regan and Willox, 2 Oct 2001).

The convenience and sophisticated of computer technology, software, scanners, color printers, and Internet resources, have made control of this growing problem of identity theft all the more challenging. The numerous threats that terrorism and crime bring to bare heighten the consequences of inaction. Technology then can be seen as both a curse and a blessing in this respect. Although the capability now exists for the villains of the world to do us harm with relative anonymity, technology also allows us the potential to imprint "unforgeable" biometric information into all forms of identification should we choose to embrace it. Countering the risks of terrorism through combating identity theft may soon be seen as a necessary investment in our future. Improvements upon current identification systems could deter this type of theft (Reuters, 17 Feb 2002). Another advantage to a secure and forgery-proof form of identification is that it will help protect the privacy of the American public by moving people away from using their Social Security numbers (SSN) for identification; once compromised for illicit purposes, SSNs can provide a host of other information about an individual (Sullivan, 3 May 2002). It is possible that a biometric driver's license for example, will evolve to double as a "smart card platform" which can be used for wide range of other identification and electronic services, from automated payments to digital signatures for e-commerce (Reuters, 17 Feb 2002).

In May 2002, two Virginia congressmen (Jim Moran-Dem. and Tom Davis-Rep.) proposed a $315 million program that would require biometric markers on driver's licenses within the next five years (Sullivan, 3 May 2002). The newly proposed license would carry the driver's retinal scan, fingerprint, or some other kind of biometric marker within an imbedded encrypted chip. The benefits of a foolproof identification system are vast. America now seems poised at the dawn of a new era in security awareness, and the

ground has become fertile for what experts see as some surrogate version of a national identity card.

3. Information Stovepipes and Disparate Bureaucracies

"Water, water, everywhere, but we have not a drop to drink." Information is almost a utility, generated in enormous volumes every second of every day. There is little argument that in this age of technology and information systems, we are drowning in information. We need timely information to carry out our daily functions, make decisions, work, plan, adjust, and respond. Yet typically, information is isolated in disparate stovepipe systems or contained within people who work in separate agencies. These systems and people often do not talk to one another; information is commonly lost within bureaucracies that cannot find it themselves inside their own systems and files.

How many times have intelligence reports of terrorist plans listing specific targets failed to prevent strikes against Americans? In 1983, we had several advanced reports of terrorists targeting the U.S. Marine compound in Beirut, Lebanon; and on 23 October 1983, 241 U.S. soldiers were killed (Gates, 20 May 2002). History can, and does repeat itself.

It should be no surprise in the post-analysis, that the clues, which would have given America notice that 9-11 terrorists were plotting a horrific attack, were in existence all along; but for whatever technical, social, or bureaucratic reasons, that information was not pieced together.

There were massive failures of intelligence that led to that terrible day on September 11th. Key pieces of knowledge were not shared with appropriate agencies and individuals. We need to learn from the past to plan for our future security effectively. Because of the extensive media reporting, some critical facts are now known; and Americans are responding by second-guessing whether we could have really prevented the terrorist plot of 9-11. The short answer is, we might have prevented 9-11. To see the system puzzle more clearly and appreciate the complexity of our intelligence systems and bureaucracy, let us examine the following 9-11 information trail:

On 5 July 2001, an FBI antiterrorism task force agent, Kenneth Williams, wrote a memo in Phoenix, Arizona, detailing the agent's discovery of a pattern of Arab men, Williams' believed to be Islamic radicals, signing up for training at flight schools (Elliott, 20 May 2002). In the memo, since known as the "Phoenix memo", Williams recommended an investigation as to whether al Qaeda operatives were training at the schools. Despite being sent to the counterterrorism division at FBI headquarters in Washington and to two field offices, including the counterterrorism section in New York, the Phoenix memo was ignored. The memo was never shared with the CIA or the White House. It was later discovered that one of 9-11 hijackers did indeed train in Arizona and had al Qaeda links (Elliott, 20 May 2002).

On 6 Aug 2001, President Bush received his daily CIA Presidential Daily Brief (PDB). The brief addressed possible terrorist threats inside the U.S. In this particular brief, he received a document, which mentioned that al Qaeda might hijack airliners and perhaps use hostages to secure the release of an al Qaeda leader or sympathizer (Elliott, 20 May 2002). According to the NSA (Condoleezza Rice), the 6 Aug 2001 PDB had no mention that a hijacked plane would possibility be flown into a building. Administration officials had conceded that turning a plane into a suicide bomb was something that nobody had considered (Elliott, 20 May 2002). If officials had made the effort to review the recent history of suicide-style terrorist plots, they would have seen that a hijacking scenario should not have been discounted.

In August 2001, the President was briefed by the CIA on the possibility that Osama bin Laden's al Qaeda terrorist network might use hijacked airliners to win concessions from the U.S. (Elliott, 20 May 2002).

On 16 August 2001, a student pilot named Zacarias Moussaoui, a man the French government knew was associated with Islamic extremists, was arrested in Minnesota on immigration charges after he aroused suspicion by apparently wanting to learn to fly jumbo jets but not land them (Arena and Lewandowski, 20 May 2002). The Federal Aviation Administration (FAA) was notified about the arrest of Moussaoui in the days leading up to the 9-11 attacks but officials said the agency decided not to warn the airlines about the possible threat because Moussaoui was already in jail (Arena and

Lewandowski, 20 May 2002). When the U.S. detained Zacarias Moussaoui, the FBI did not share information of the possible threat with anyone in the White House's Counterterrorism Security Group (CSG) (Elliott, 20 May 2002). Moussaoui has since been charged with complicity in the 9-11 attacks.

After 9-11, the White House made a conscious decision not to disclose the August briefing, hoping that it would be discussed "in context" many months later, when congressional investigations into the attacks eventually got under way (Elliott, 20 May 2002).

President Bush's national security aides had been warned during the presidential transition that there was an al Qaeda presence in the U.S., but prior to 9-11, fighting terrorism had not been a top priority in the early months of the Bush Administration (Elliott, 20 May 2002).

There were earlier warning signs of the type of assault America could face. The paradigm of systems and bureaucracies which do not talk to one another reveals itself further when in 1995, authorities in the Philippines foiled a mass hijacking plan, masterminded by Ramzi Yousef, whereby American planes were to be hijacked and blown up over the Pacific (Elliott, 20 May 2002). Yousef was also notoriously known for plotting the 1993 World Trade Center bombing (Elliott, 20 May 2002). More evidence of the potential for an air attack against America was discovered during the investigation of Yousef and his partner, Abdul Hakim Murad. The subsequent analysis uncovered a plan to crash a plane into CIA headquarters in Langley, Virginia (Elliott, 20 May 2002). If this were not enough to prod the imagination, in 1994, French intelligence authorities discovered and foiled a plot by the Algerian Armed Islamic Group to fly an airliner into the Eiffel Tower (Elliott, 20 May 2002). Despite the historical leading indicators, no one in the Bush Administration compiled this available threat intelligence information; and subsequently, the U.S. was surprise that such a tactic of mass murder might be a possibility. In fact, up until the 9-11 terrorist attack, FAA security policy for airline crews dealing with hijacking remained "cooperate with hijackers' demands" (Arena and Lewandowski, 20 May 2002).

The Phoenix memo had not been shared with the CIA, the Senate Intelligence Committee, White House, and President (Elliott, 20 May 2002). Had the President's brief writers been aware of it somehow, the 6 August 2001 PDB would have at least attracted more discussion. While it certainly appears some of the pre 9-11 intelligence did look like an obvious smoking gun, it is far more difficult than it seems to package together the sometimes incomplete or ambiguous information and form compelling analysis, worthy of convincing higher government authorities enough to prompt complex and high-risk decisions (Gates, 20 May 2002).

One of the major shortcomings of our existing intelligence information systems is that it is run by individuals who, for a variety of reasons, are overwhelmed, distracted, or are otherwise confused by volumes of "potentially useful" information that comes their way. Information that is supplied often arrives too late for a proper staffing and analysis. When confronted by hundreds or even thousands of seemingly worthy pieces of intelligence information, an overworked and understaffed department may be forced to prioritize, and a key piece of information may go unnoticed in the downpour of data. People are often molded by outdated perceptions of the way the world should be or by existing models of their work process, which may be ingrained in decades of institutional tradition. We should learn from this experience and reexamine our existing methods of information exchange. We should capitalize on the ingenuity of our out-of-the-box thinkers, rewarding adopted ideas for improvement, and encourage the utilization of smart technologies where practical.

Fixing a complex and bureaucratic system that desperately needs improvement is a great challenge, and it will not happen overnight. The weaknesses in our national security system were revealed to the world after 9-11. Sharing timely information among those who need it is key. One could easily argue that had authorities tried to track down all Muslim flight-school students, they would have been accused of racial profiling. Undeniably, True. Changing the way in which government agencies do business, and eliminating the things that contribute to discourse and inter-agency rivalry is also a monumental, but necessary task. It is inevitable that some rights may be infringed upon as government seeks to protect the public. One cannot help but wonder how much

sacrifice in privacy does America wish to pay in order to feel safe. One FBI agent who prefers to remain anonymous, answered this question quite bluntly; he said:

> The public expects FBI agents to use instinct to surgically extract terrorists from society; and to do it without inconveniencing the public or infringing on innocent lives. Americans have unrealistic expectations about what law enforcement can do in a society in which personal freedom is deemed more important than public safety. Americans say they will give anything to be safe from terrorists. They don't really mean it. They would rather live in a free society than be completely safe. That means some dots won't ever be connected. (CNN, 20 May 2002).

During a recent commencement speech to the U.S. Naval Academy Class of 2002, Vice President Dick Cheney emphasized America's need to go on the offensive to eradicate terrorist networks where they live. He said the terrorists are working to acquire the deadliest of weapons, and that another strike against the U.S. is almost certain (CNN, 24 May 2002).

It is apparent to military strategists that Cold War intelligence gathering systems are not effective in this new war on terror. They did not envision an enemy living in Afghan caves one day, and moving to European and American apartments the next, blending into society, and stealthily infecting peaceful civilization with plots of death by surprise, sabotage, and deception (Elliott, 20 May 2002). We now live in a world where criminals are as powerful as countries; and some countries are run by criminals (Elliott, 20 May 2002). The way we collect, analyze, and share information on an enterprise level must change to meet the needs of our new defense strategy.

Creating smarter systems has as much impact on our ability to effectively share information as does repairing our disparate bureaucracies. The terms: pattern-recognition, data mining, intelligent networking, neural networks, intelligent algorithms, expert systems, decisions support systems, smart systems, and knowledge management, all come to mind when one thinks of building a better system for alerting authorities of impending danger or suggested actions to be taken. We are not merely talking about computers systems now; we are talking about managing information and transforming it into knowledge in such a way, that it becomes powerfully synergistic. This is relevant to surveillance and biometrics technology because the once-rival intelligence and police

agencies around the world now need to share and analyze information quickly (Patton, 1 Feb 2002). Many surveillance systems in the U.K., for example, are watched not by people but by software algorithms that query authorities if attention is required on a particular event.

According to Homeland Security Director Tom Ridge, we need interoperable communications systems and a national surveillance network to assist with everything from border security and information sharing to bioterrorism and first responders (Porteus, 24 Apr 2002). We need to have more organized background information about who is coming through our borders; we need to know when they arrive, how long they stay, where they are, and what they are doing. If someone is on a "wanted list," we need to know that. If someone is using a false identity, we need a system that will alert us of that. If a visa is expired, we need to know that automatically. If someone is trying to smuggle in hazardous materials, arms, or WMD, we need a system that will help our law enforcement authorities to alert to that threat. Our communications systems must be designed such that when a pattern of unusual events begins unfolding such as a pandemic medical crisis, our first responders, and medical teams can quickly react to keep the threat from spreading and harming others.

For agencies to exchange vital information with other agencies, they must first be committed to "want to" share. This is a cultural barrier that goes far beyond technology; in fact, it should be a prerequisite to employment of technology. Members of the FBI, CIA, DEA, IRS, and Customs Service have had long running interagency rivalries. Secrecy, mistrust, and budgetary power plays historically damaged any chance of improving information exchange among agencies. Any temporary cohesion gained out of responding to a crisis usually diminished again over time (Patton, 1 Feb 2002). Moreover, it is not always people but legal guidelines that limit interagency information exchange. Intelligence and law enforcement agencies are not always permitted by law to share information. This too must change. This is even more profound on an international level when you are looking at laws between neighboring countries. It gets complex since each country has different extradition laws and treaties, leading to inevitable disagreements as countries pursue suspected terrorists across borders. To smooth out

these judicial procedures, the European Union earlier in 2002 created the European Judicial Cooperation Unit, EUROJUST, based in Brussels, Belgium, which brings magistrates together from different countries to cooperatively resolve differences (Patton, 1 Feb 2002). Europe is proving that most of the information sharing barriers are often political and easily workable through increased collaboration.

Until the recent passage of the new antiterrorism bill, the FBI had not been allowed to reveal anything obtained during domestic criminal investigations with the CIA (Patton, 1 Feb 2002). Communications between intelligence agencies is now a requirement. The antiterrorism bill also authorizes the FBI to share its data with the State Department and the Immigration and Naturalization Service (INS). Lawmakers are also busily preparing additional legislation that will encourage information sharing and finally eliminate stovepipe information barriers.

Once these bureaucratic barriers are crossed, the technology can be pivotal in making the information flows happen. There are a few success stories that provide models for various intelligence agencies in information sharing using private networks and secure Internet systems. For example, Interpol, the European-based law enforcement and intelligence network, is made up of 179 countries and has served as a hub for international law enforcement cooperation since its inception in 1923 (Patton, 1 Feb 2002). Interpol serves as a coordinator or liaison for the information flow. Each country owns its own databases; Interpol merely serves as a central clearinghouse for international law enforcement cooperation.

Even with the assistance of technology and the many corporate vendors waiting to help, the global transformation will not be straightforward. Technology integrations can be extremely complex because of the uniqueness of different agency systems. Federal, state, and local agencies face the daunting challenge of interconnecting hundreds of unrelated databases, each running on different hardware platforms using different operating systems and running dissimilar software suites. Many of these departmental systems were purchased without any coordination with other agencies, making the cost and complexity of effort in linking them all the more challenging. Fortunately, federal funding is coming to assist in the effort. The administration has allotted $15 billion for

information technology in the proposed fiscal 2003 budget, with $4 billion of that going for IT security (Porteus, 24 Apr 2002).

The ultimate goal is to link all of the major databases of U.S. intelligence, DoD, and police agencies into a single virtual intelligence network; but this will take many years. In the short-term, we can at least use the Interpol sharing model and expand upon its information sharing capabilities.

On a U.S. national level, several interagency communications models do exit. For example, the military's Secret Internet Protocol Router Network (SIPRNET) is used to share classified and intelligence-related information among services and intelligence agencies.

Another information sharing model is JNet, which Homeland Security Director Ridge pushed during his term as governor. It is a web-based network linking data from various law enforcement agencies, which provides thousands of photos of criminal suspects. Similarly, the U.S. government is investigating building its own Internet, called GovNet, to provide safe transmission of sensitive data and government communications (Patton, 1 Feb 2002).

Intelink is also an existing effort to create a shared information environment for the intelligence community. Intelink serves as a giant intranet for intelligence analysts in the National Security Agency (NSA) and the CIA, allowing analysts to share information in various classified levels.

In 1996, the Defense Advanced Research Projects Agency (DARPA) began work on a pilot project, called Genoa, a peer-to-peer computing network designed to allow for interagency data sharing. The concept is for high-level intelligence analysts to share information and patterns of criminal behavior. The National Security Adviser has recently proposed using Genoa to foster information sharing among agencies (Patton, 1 Feb 2002).

The concept of knowledge management and interagency cooperation in law enforcement and intelligence dates back to 1974 when the DEA set up the El Paso Intelligence Center (EPIC). Intelligence analysts, criminal investigators, and support

personnel from numerous federal agencies and two state agencies staff EPIC. Their purpose is the hosting of intelligence from various federal databases, as well as their own. Most state police can contact EPIC to find out information about drugs or illegal aliens, and most notably, EPIC is now being used to assist in counterterrorism investigations (Patton, 1 Feb 2002).

Information sharing models such as SIPRNET, Intelink, and EPIC, show that agencies can share data if there is an infrastructure established with a specific purpose in mind (Patton, 1 Feb 2002). The battle to recast the legacy stovepipe information systems into knowledge sharing portals will be a difficult but attainable goal. It must begin with changing the culture of people within each agency, and that includes providing effective leadership and focus on the road ahead. It also means embracing biometric authentication, sensing, and surveillance technologies to accurately obtain credible information that can be digitally managed by fast and efficient systems. Once the technological infrastructure is established and personnel are trained in the new processes, utilities such as data mining, pattern recognition, and decision support will become available on a more effective level. In the future model, managers will need to ensure incentives are built-in to encourage continued sharing of knowledge. The technology is not a panacea, but a means to maximize human intelligence and transform information into decisions and actions that will assist in our prevailing over terrorism and other criminal activity.

III. NATIONAL STRATEGY FOR HOMELAND SECURITY

A. THE CHALLENGE

The concept in establishing an office for homeland security serves to provide the United States with a coordinating agency that will be responsible for leadership oversight in managing federal, state, and local security, and defense responses. Our nation has never had a blueprint for a national strategy to fight war on terrorism (Whitehouse, 2002). This is a new concept for the United States. Security of our homeland, especially security against terrorism, has become an inescapable part of life in the 21st century. Americans were incapable of comprehending the likelihood of the 9-11 attack. After the initial shock and subsequent resolve to respond, we are now rethinking our entire approach to operating in this new world. There are many issues that must be addressed for developing homeland security; it is a task of monumental scale and complexity. Reaching our objectives will require hard work and a sustained investment of resources over many years. Unfortunately, this is a mission that will have no end.

The challenges ahead for the newly created Office of Homeland Security are multidisciplinary and will involve numerous agencies from all levels of government. The plan to realize the goals of homeland security and maintain a certain level of defensive posture must be tempered with a balance for quality of life and a sense of cost-effectiveness (USCNS, 15 Feb 2001). The road to achieving the new agency's goals has become an investment for the preservation of the civilized world.

This chapter will discuss the strategy of the Office of Homeland Security and define the vital supporting role that technology and people will be asked to play in the months and years ahead.

B. MISSION OF HOMELAND SECURITY

The mission of the Homeland Security Office is to develop, coordinate, and implement a comprehensive national strategy to secure the United States from terrorist threats or attacks (Whitehouse, 28 Feb 2002). It is a multi-layered concept of actions among federal, state, local, private, and individual citizens to deter, defend against, or

mitigate attacks within the United States, and to respond to other major domestic emergencies (ANSER, 28 Feb 2002).

C. THE STRATEGY

The strategy of the homeland security is based in three underlying themes. First, government leadership must define a clear vision for homeland security in cooperation with all appropriate partners and muster the necessary resources to get the job done. Second, a detailed national homeland security strategy should be developed based on a comprehensive assessment of national threats and vulnerabilities. Third, the great number of organizations that will be engaged in homeland security need to have clearly articulated roles, responsibilities, and accountability mechanisms (GAO, GAO-01-1158T, 21 Sep 2001).

The current homeland security strategy is a work-in-progress. Guidelines for the formation of a homeland security strategy are provided in the Homeland Security Strategy Act of 2001, House Resolution 1292 (Library of Congress, 29 Mar 2001), and the Office of Homeland Security Act of 2001, House Resolution 3026 (Library of Congress, 18 Mar 2002). Components of the strategy from the above-mentioned legislation include the following (H.R. 1292 and H.R. 3026):

> (1) A comprehensive research, development, and procurement plan for supporting homeland security.
>
> (2) Mechanisms to insure the flexibility and mobility in federal personnel policies and practices to achieve maximum effective use of personnel among all concerned agencies.
>
> (3) Policies and procedures to maximize the collection, analysis, translation, exploitation, and dissemination of information throughout federal, state, and local government.
>
> (4) Plans for improving the resources of, coordination among, and effectiveness of health and medical sectors for detecting and responding to terrorist attacks on the homeland.
>
> (5) Provide for augmentation of existing medical response capability and equipment stockpiles at the Federal, State, and local levels.
>
> (6) Specific measures to enhance cooperative efforts between the public and private sectors in protecting homeland security.

(7) Identification of explicit homeland security threats based upon the results of a comprehensive risk assessment.

(8) Development of specific guidance for antiterrorism and consequence management activities as well as detailed objectives that provide measures of effectiveness.

(9) Identification of the federal executive departments, agencies, and other organizations that should play a functional role in homeland security.

(10) Provide for the selective use of personnel and assets of the Armed Forces in circumstances that their unique capabilities could be used without infringing on civil liberties.

(11) Optimization of the use of intelligence capabilities, including improvement of processes by which intelligence information is provided to State and local governments.

(12) Development of a multiyear plan for phased implementation of the overarching strategy and a comprehensive projected budget (H.R. 1292 and H.R. 3026).

These national homeland security strategies are long-term initiatives. The goal is to prioritize implementation in workable stages. The strategy will be based on partnership with state and local governments, the private sector, and citizens (Whitehouse, 2002).

A multi-year federal budget preparation process will support the overall national homeland security strategy. The plan calls for expenditure of monies only after proper analysis has been done to ensure that funds will be spent wisely. Additionally, new and expanded Federal programs will aim to reorganize government at all levels—reforming legislation, providing tax incentives, cost-sharing, and developing cooperative arrangements with the private sector and citizens (Whitehouse, 2002).

The homeland security plan will create emergency management and medical systems, which are better able to respond to terrorism, diseases, and mass casualties of every type. It also seeks to build a broader management system that is more adept at filtering for terrorists as well as providing for the improved flow of lawful human traffic (Whitehouse, 2002).

The strategies aim to set clear, attainable objectives for homeland security, which include benchmarks and other performance measures by which progress and resources can be evaluated. The strategy will take into account the existing institutions and systems for providing homeland security, such as law enforcement, public safety, public health, and emergency management. Redundancies will be eliminated and complementary responsibilities will be linked for collaboration. Individual agencies' responsibilities and authorities for homeland security will be clearly and logically aligned with their core competencies. The plan will build upon systems and processes that currently work well together and are logically organized, improve on others that require attention, and eliminate those that are detractors (Whitehouse, 2002).

D. COMPONENTS OF THE HOMELAND SECURITY BUDGET PLAN

The importance of funding the continued protection of America's critical resources is vital. This is especially important because we are a technology-dependent nation. Technology is what will help us gather, analyze, and share intelligence information among appropriate agencies. Funding of technology and other programs is key to enabling the effectiveness of homeland security. The emerging Presidential Budget priorities have been aligned with national strategies for homeland security that include plans for information infrastructure, physical infrastructure, transportation and commerce, as well as law enforcement and intelligence. Homeland security budget history and apportionment by area are provided in Figure 3.1 and 3.2 for reference.

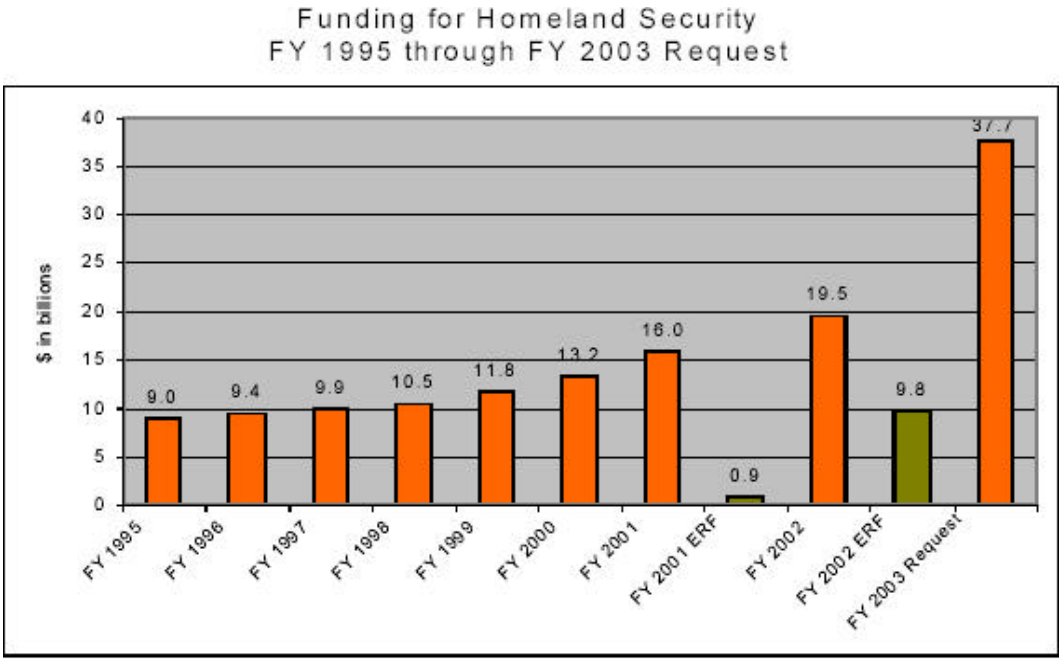


Figure 3.1. Homeland Security Funding FY1995-FY2003. (From: Whitehouse, 2002).

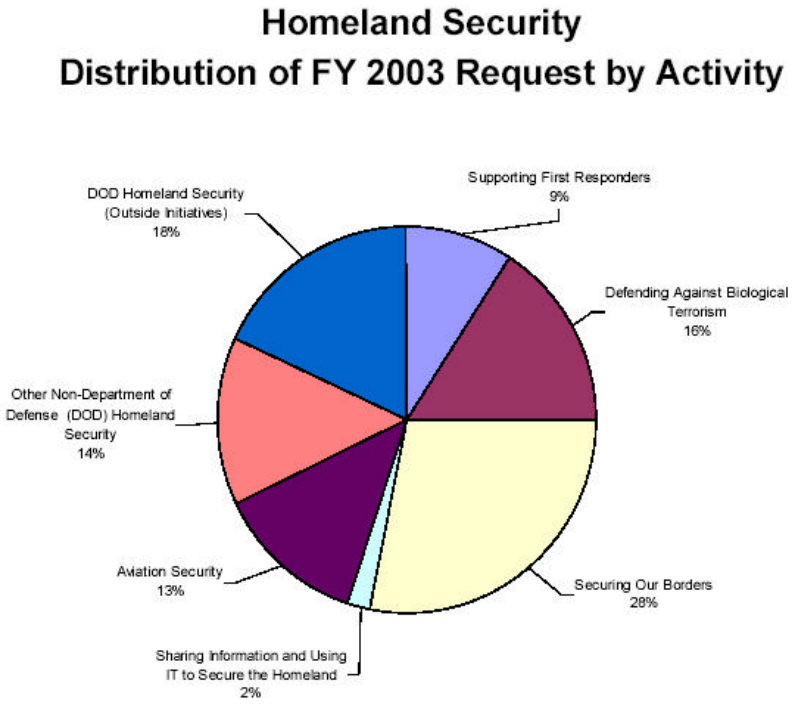


Figure 3.2. Homeland Security Funding Distribution, FY2003. (From: Whitehouse, 2002).

Here are some specific programs from the proposed FY2003 Homeland Security budget:

1. Homeland Security Budget Priorities

The following key initiatives will be included in support of the homeland security agenda and funded under the President's Budget for FY2003:

a. Transportation Security

The President's Budget for 2003 requests $4.8 billion to fulfill aviation security authorizations established under the November 2001 Aviation and Transportation Security Act (TSA). The plan calls for a phased program of vitally important milestones toward achieving a secure travel system (Whitehouse, 2002). Air, rail, highways, bridges, and other transportation assets are critical to our economic and national security (Whitehouse, 2002).

b. Federal Law Enforcement

The 2003 budget will enable the FBI to add over 300 special agents and investigative staff for surveillance of terrorists operations and related intelligence. The funding will also add more than 130 FBI special agents and 25 DEA agents wholly dedication to combating cyber-crime and drug money laundering, as well as protecting our banking, finance, utility, energy, and transportation systems from disruption by terrorists or other criminal acts. The resources will help provide special financial crime investigators who are adept at identifying and shutting down the sources of money that support terrorist cells (Whitehouse, 2002).

c. Citizen Corps

The budget for 2003 provides $144 million in matching funds to support the formation and training of local Citizen Corps Councils. The Citizen Corps is designed to enable Americans to volunteer their skills and abilities in participation of homeland security activities in their own communities. The community-based Citizen Corps Councils develop action plans, assess possible threats, identify local resources, and coordinate with other Citizen Corps programs. The budget further provides more than $230 million for these related Citizen Corps programs, including Volunteers in Police Service (VIPS) Program, Medical Reserve Corps, Operation TIPS (Terrorist Information

and Prevention System), Community Emergency Response Teams (CERT), and Neighborhood Watch Programs (Whitehouse, 2002).

d. Department of Defense and Intelligence Community

The 2003 budget requests $7.8 billion for homeland security-related activities of the Department of Defense and Intelligence community, of which $4.6 billion is dedicated to physical security of stateside DoD facilities and personnel. The remaining $1.3 billion is dedicated to supporting combat air patrols within U.S. airspace. Significant funding for counter terrorism research and development and specialized WMD response teams are also provided (Whitehouse, 2002).

e. Critical Infrastructure Protection

Since the 9-11 attack, the Administration provided broad and decisive measures to defend the highest risk targets and critical infrastructure systems. These high-risk assets include nuclear power plants, seaports, hydroelectric dams, telecommunications nodes, border crossings, and chemical facilities. This endeavor requires the close cooperation and involvement of many State and local agencies and private companies. The systematic process of defining and prioritizing our Nation's efforts will provide further framework for unified critical infrastructure protection plan (Whitehouse, 2002).

2. Information and Infrastructure Protection

a. National Infrastructure Protection Center (NIPC)

The National Infrastructure Protection Center is the nation's principal cyberspace-threat detection and response center located within the FBI. They are responsible for protection from both physical and cyber attacks. The President's Budget for 2003 requests $125 million to fund the center. The budget request reflects an increase of more than $50 million from the NIPC's previous year's funding level (Whitehouse, 2002).

b. Cyberspace Warning Intelligence Network (CWIN)

The Cyberspace Warning Intelligence Network is designed to respond to Internet-based program attacks. The CWIN mission is to link the major agencies in government and the private sector for improved coordination response to future cyber

attacks or Internet crisis. The budget for 2003 calls for $30 million to create the CWIN (Whitehouse, 2002).

c. Priority Wireless Access (PWA)

In times of a major crisis, wireless communication channels can jam due to congestion, preventing first-responders from making calls in a timely manner. The 2003 budget requests $60 million to develop a wireless priority access program that will give authorized users priority on the cellular network (Whitehouse, 2002).

d. National Infrastructure Simulation and Analysis Center (NISAC)

The 2003 budget requests $20 million to fund the National Infrastructure Simulation and Analysis Center at the Department of Energy. The center will support and foster partnerships between Federal and private research sector efforts to understand the dependencies between the Internet, our critical infrastructure, and our economy (Whitehouse, 2002).

e. Secure "GovNet" Feasibility Study

The government must make its information systems secure against intruders and attacks. The 2003 budget requests $5 million for a feasibility study for developing a government network (GovNet) that will provide a secure environment for top government information exchanges (Whitehouse, 2002).

f. Advanced Encryption Standard (AES)

The President is supporting Federal agencies in acquiring new and improved computer security standards for information transfer. The Advanced Encryption Standard has become a Federal standard designed to protect sensitive and unclassified information well into this century. The standard is also expected to find wide use in the business and consumer markets (Whitehouse, 2002).

g. Cybercorps Scholarships for Service (CSS)

The budget for 2003 requests $11 million for the "Cybercorps Scholarship for Service" program. By providing scholarship funding to universities across America, the CSS program encourages college students to become information technology security professionals within government. Under the managed of the National Science

Foundation and Office of Personnel Management, this program also promotes the creation of computer security academic programs at universities (Whitehouse, 2002).

E. HOMELAND SECURITY REORGANIZATION AND RESOURCES

The notion of Homeland Security (HLS) is not new to Americans. America addressed homeland defense and organizational restructure after Pearl Harbor. In December 1945, shortly after America's victory in World War II, President Harry Truman had Congress combine the War and Navy Departments into a single Department of Defense. The idea was to organize for collaboration and for an effective fighting force capable of protecting the Nation. This goal was achieved with the National Security Act of 1947 and its subsequent amendments in 1949 and 1958. The resulting reorganization integrated the separate military Departments into the Department of Defense with a civilian secretary solely in charge. It also created a Central Intelligence Agency to coordinate all foreign intelligence collection and analysis. The National Security Council was also established to manage foreign and defense policy efforts. Additionally, briefings to the Secretary of Defense by an expert panel of biological weapons experts emphasized the need for a vision of homeland defense (McIntire, 2002).

The next time the term homeland defense was examined was in 1997 when Congress mandated post-Cold War reformation of the Department of Defense. Congress mandated an internal "Quadrennial Defense Review" (QDR) of military strategy, which looked at how defense was organized and prioritized. A subsequent National Defense Panel (NDP) then reported its conclusions that terrorism and related threats to the United States were becoming increasingly likely. In the years that followed, other reviews came to similar conclusions, and the term "Homeland Defense" became popular just long enough for it to be renamed "Homeland Security" — encompassing a meaning beyond defense. Homeland Security represents all the measures necessary for government and private agencies to collaborate in the actions and initiatives toward protecting the homeland. As a subcomponent of homeland security, DoD was predetermined to be an adjunct first-responder to support domestic requirements during disasters and law enforcement crises. This DoD "Civil Support" role implies that the military may be

asked to provide support within the United States for responses that have nothing to do with foreign attack (McIntire, 2002).

The role of homeland security is purposefully broad and is presently undergoing a transformation that is being shaped by the chronology of U.S. responses to the 9-11 attack (Appendix A). Homeland security responsibilities are currently shared with over a 100 governmental agencies. A new structure was imminent. The much needed reorganization plan was delivered in June 2002, and the "Office of Homeland Security" became the "Department of Homeland Security" (Appendix B). The lessons learned since 9-11 has shown that for HLS to be most effective, it must be fully funded as a department with budget and control authority, and have a Cabinet appointed leader with power to direct. Previously, the Director of Homeland Security had only advisory privileges to the President and a meager staff to coordinate dozens of agencies over whom they had no real control (Appendix C). History continues to teach us that significant security challenges require clear lines of responsibility and the combined efforts of the government agencies. History further reveals that new challenges require new organizational structures (Whitehouse, June 2002). The HLS Department is ripe for such reorganization.

Under the new plan, the Department of Homeland Security would have a clear, efficient organizational structure with four divisions (Appendix B):

(1) Border and Transportation Security;

(2) Emergency Preparedness and Response;

(3) Chemical, Biological, Radiological, and Nuclear Countermeasures; and

(4) Information Analysis and Infrastructure Protection (Whitehouse, June 2002).

Even after establishment of the new department, homeland security will still involve the efforts of the many Cabinet-level departments that have jurisdiction in the dozens of areas under their purview (Appendix D). Furthermore, HLS will continue to provide interagency coordination and be the advisor to the President on homeland

security related issues (Whitehouse, 2002). The ultimate mission of this new Department is to utilize the resources of America to keep our way of life free from terror.

F. TECHNOLOGY AS LEVERAGE IN DEFENDING THE HOMELAND

In recent statements to the Electronic Industries Alliance annual conference, current homeland security director Tom Ridge made it clear that homeland security depends on new technologies. The director more specifically mentioned the importance of biometrics and surveillance technologies, including next-generation detection devices designed to find trace amounts of chemical or biological agents (Porteus, 24 Apr 2002). He further pointed out that technology supports all of the administration's homeland security efforts: border security, information sharing, counter-terrorism, and first-responder emergency support. The importance of technology is paramount to verifying authentication of individuals, controlling our borders, and monitoring movement of commerce and human traffic. Surveillance and biometrics are among the arsenal of sensor technologies capable of capturing and collecting vast amounts of intelligence information. "Yes, it is a new world, but it is a world in which technology is suited to play a very critical role," Ridge said (Porteus, 24 Apr 2002).

Depending on which side of the homeland security argument one takes, biometrics, surveillance, and information technology can appear infringing on civil liberties, while on the other hand actually protecting the rights of Americans to live free of terror. The dilemma is one that has continuous attention at the Homeland Security Department. In defending the goals of homeland security, Attorney General John Ashcroft, in a testimony before a Senate subcommittee on the government's ability to combat terrorism said, "We're not destroying rights. We're protecting rights. I believe the American people deserve to have their rights protected" (Klein, p. 6).

The funded technology portion of Homeland Security is quite large. In the $37.7 billion slated for Homeland Security proposed in the fiscal 2003 budget, $15 billion is allotted for information technology while $4 billion of that goes to IT security (Porteus, 24 Apr 2002). The message seems clear that technology is well supported as a resource. The civil liberties watch keepers should also be appraised that emerging legislation is a positive feature helping to integrate and balance technology into our homeland security

strategy for the 21st century (Porteus, 24 Apr 2002). In the next two chapters, we will examine closely the specialized technologies supporting homeland security and discuss their unique applications.

IV. UBIQUITOUS SURVEILLANCE AND BIOMETRICS TECHNOLOGY

A. VIDEO SURVEILLANCE AND VIDEO FORENSIC TOOLS

Since the 1980s, security cameras have increasingly been installed at public areas, such as ATMs, intersections, transportation centers, department stores, campuses, packing lots, corridors, and stadiums (Petersen, pp. 8-51). Since 9-11, video surveillance has grown dramatically. The threat of additional terrorism has made the use of surveillance technologies in the United States inevitable. One only needs to visit New York City and Washington D.C. to see its new implementations. At these locations, the U.S. has used the United Kingdom (UK) as a model to develop its system. Similar surveillance systems are being employed at other high threat locations and events. Part of the video surveillance infrastructure already exists in many areas of our country and could be leveraged to expand the evolving surveillance grid. Most of the surveillance systems in the U.S. are privately owned and are made up of products similar to those shown in Figure 4.1.

CCTV *Infrared* *Bullet Camera Systems*

Figure 4.1. Video Surveillance Equipment. (After: 123CCTV.com, 2002).

Although cameras are the first technology we think of when we imagine surveillance, cameras are merely one of the many layers in an ideal ubiquitous surveillance network. Technologies such as video forensic tools, “smart” cameras, and facial recognition play important roles.

New advances in digital video and video forensic tools (like Sarnoff Corporation's VideoDetective) and various products from companies (such as Avid Technology and Ocean Systems) provide agents with new methods to extract clear pictures of surveillance scenes and suspects from poor-quality images. By digitizing analog video images and processing them through PCs, video tapes can be stabilized so that it is easier to follow a suspect in a video clip, extract license plate numbers hidden in shadows, filter out rain and snow in a background to have a better view of an image scene (see Figure 4.2.)(Sarnoff, 1 Apr 2002 and Avid, 19 Jun 2002).

Figure 4.2. Video Forensic Tools. (After: Sarn.off, 1 Apr 2002 & Avid, 19 Jun 2002).

The use of "smart" cameras can aid in monitoring large government or public areas that are considered potential terrorist targets. The Sarnoff Corporation, located in Princeton, N.J., has developed advanced video microprocessors that along with developed computer algorithms could allow security cameras to monitor an area, recognize suspicious behavior, focus on it, and send an alert if any action is deemed dangerous (Sarnoff, 1 Apr 2002).

Non-intrusive biometric technologies, such as facial recognition, gait recognition, and thermal facial-scans, can be used to aid in developing an effective ubiquitous surveillance system, which link cameras at security checkpoints with government databases of suspected terrorists via the Internet.

B. BIOMETRICS

Technologies involving physiological and behavioral adaptations can come to play a major role in proposed ubiquitous surveillance systems and smart card technologies. Biometrics is the science of automatically identifying individuals based on their physiological or behavioral characteristics. It has emerged as a viable solution for a

range of applications, and its use as a tool should be strongly considered in this new "age of terror."

Prior to 9-11, biometric technology was limited in use. The overall market for biometrics was approximately $325 million in 1999 (Evangelista, 21 Feb 2000). Until recently, biometric technologies were slow to catch on because of the high cost and enormous computing power required to build accurate systems. However, the combination of the growth in PC computing power, evolution of proprietary adaptive algorithms, lower-cost infrared optics, and improved measurement methods have enabled manufacturers to create biometric devices for mainstream applications at a lower cost. Biometric technologies are now emerging as a practical, effective solution for law enforcement, security, and fraud-free e-commerce. It is also preventing identity theft and attendance fraud. The following are some startling statistics that explain the evolving use of biometric technologies:

- Approximately $1 billon in welfare benefits in the United States are annually claimed by welfare recipients who "double dip" with fraudulent multiple identities.
- Master Card has estimated credit card fraud at $450 million per year based on charges made on lost or stolen credit cards.
- Cellular bandwidth thieves, many who use stolen PINs or cellular phones, make approximately $1 billion worth of cellular telephone calls annually.
- Approximately $3 billion per year is lost due to ATM related fraud.
- Billions of dollars are misappropriated due to fraudulent encashment of checks each year (Jain, p. 2).

In this new "terror age," the biometric market will surely grow exponentially as government agencies and public sectors investigate its further use to solve security and law enforcement problems. According to industry analysts, the worldwide biometrics market will reach $10 billion by 2003 (I/O Software, Jun 2002). It will be deployed where identification and authentication is required. Today biometric devices control access to many computers, ATMs, secured rooms, vaults, research laboratories, prisons, transportation centers, and military installations.

1. Biometrics Overview

a. Identification and Authentication

Both government agencies and the public sector are increasingly recognizing the limitations of picture IDs, paper documents, passwords, and PIN numbers as identity theft, computer hacking, cyber crime, and terrorism become more prevalent (Polemi, p. 3). Identity theft or fraudulent identification can lead to security breaches that result in unauthorized access to secure or restricted areas such as airport handling areas, military installations, laboratories, nuclear power plants, water reservoirs, and the secured networks that make up our critical cyber infrastructure (Polemi, p. 5).

The two types of security processes that can be used to counter these threats are identification and authentication. Identification is the process whereby an identity is assigned to a specific person. Authentication is verifying an individual's identity. Authentication procedures are based on the following premises:

- Proof by Possession (lowest level of security): what the person owns, such as a smart card without biometrics or a photo ID.
- Proof by Knowledge (second level of security): what the person knows, such as a password or PIN.
- Proof by Property (highest level of security): what the person is or does, behavioral or physiological biometrics (Dysart, 1998).

Traditional technologies that are based on the first two premises of authentication are not sufficient to reduce the impact of counterfeiting or fraud. Smart cards can be lost or stolen. Fraudulent photo IDs can be fabricated. Passwords can be lost, cracked, or obtained using social engineering. Biometric technologies provide the highest level of security because they verify physiological or behavioral characteristics that are unique to each individual and are difficult to disguise or falsify (Polemi, p. 5). They are more reliable and are more capable in distinguishing between a specific person and an impostor than any other type of identification technique. They provide the additional, convenient security barriers that are required as we evolve into a more secure society and become even more computer-dependent. The use of biometric devices also provides user-convenience because users do not have to deal with remembering passwords or having to reset them periodically (Polemi, p. 5).

During identification (see Figure 4.3) a biometric system tries to answer the question "Who is this?" and establish whether a biometric record exists for that individual. This process is often referred to as between subject variability (1:N). If it does, it will attempt to identify the person whose sample was matched. Verification is a one-to-one comparison. During verification (see Figure 4.3) the biometric system tries to answer the question "Is this person who he or she claims to be?" and attempts to verify the identity of someone, for example, who is using a smart card (I/O Software, Jun 2002). This process is often referred to as within-subject variability (1:1).

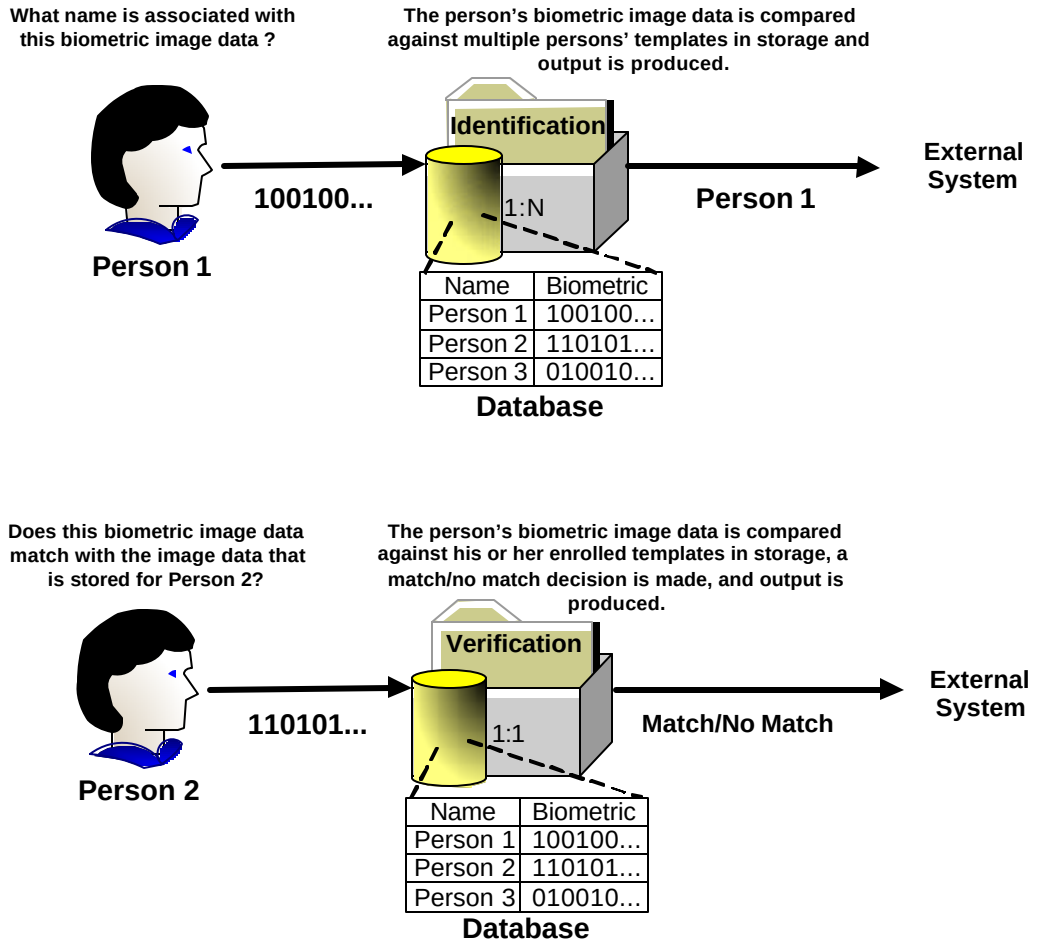


Figure 4.3. Identification and Verification Processes. (After: Nanavati, p. 11).

It is desirable for a biometric technique to have maximal between-subject variability but minimal within-subject variability. The number of forms of variation, degrees of freedom, which are spanned by the biometric patterns determine the relationships between the two types of variability (Jain, p. 103). It is also desirable for recognition decisions to be based upon features that allow for the identification between even genetically identical or related individuals.

b. Biometric-Based Systems

The most popular physiological biometric techniques are iris scan, retina scan, fingerprint verification, hand geometry verification, and facial recognition. The most popular behavioral biometric techniques are signature verification, voice verification, keystroke recognition, and gait recognition. Lesser commercially deployed or new biometric methods include DNA pattern, vein pattern, ear recognition, odor/scent identification, thermal face-scan, subcutaneous hand-scan, sweat pores analysis, and fingernail bed identification.

Biometric-based systems rely on a wide range of technologies and algorithms to operate. Figure 4.4 illustrates the typical operating subsystems that make up a biometric system.

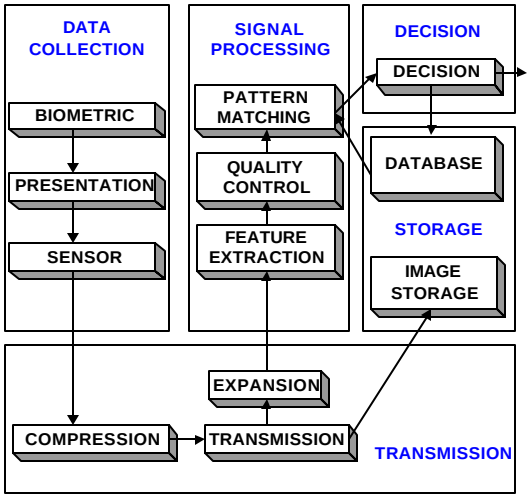


Figure 4.4. Generic Biometric System. (After: Jain, p. 348).

In the *Data Collection* subsystem, a biometric characteristic is presented to the system's sensor, and a pattern image of the biometric characteristic is captured. This process occurs in both the initial enrollment and in the identification and verification processes (Jain, p. 347). During the enrollment process, some biometric technologies may require additional samples to be obtained in order to build a useful profile of the biometric characteristic (I/O Software, Jun 2002).

In the *Transmission* subsystem, the unique biometric features are converted into a signal representing the biometric pattern and are compressed, transmitted, and expanded. Noise may be inadvertently added during this process (Jain, p. 347).

In the *Signal Processing* subsystem, stable, unique features are extracted from the received signal and converted by the system into a mathematical code that is then either stored as a template or compared to templates already stored in *Storage* (Jain, p. 347). A biometric template is a mathematical representation of a person's unique biometric characteristic stored in digital form. By itself, the template is of no use. It cannot be used to reconstruct a biometric image pattern to allow a person to be identified as someone else (I/O Software, Jun 2002).

In the *Storage* subsystem, the templates derived from the image features are stored. Storage could also include the raw signals received from the *Transmission* subsystem. Templates can be stored in different places depending on the security requirements of the application. The templates can be stored in the biometric device, in a central database, or in smart cards. When storing templates in a centralized database, Trusted Third Party (TTP) services provide security in transmitting and managing the templates (I/O Software, Jun 2002).

In the *Decision* subsystem, accept or reject decisions are made based upon the signal processing system's policy and the comparative scores received (Jain, p. 348). The biometric system attempts to verify an individual's identity by comparing the new biometric sample captured with the previously stored template. If the two samples match, the biometric system confirms the applicant's identity. Because both physical and

behavioral biometric characteristics may change slightly over time as we age or become scarred, the biometric system must allow for subtle changes in these biometric characteristics. To allow for these minute changes of a person's biometric characteristics, a threshold or error tolerance is built in within the decision subsystem set. Comparison between the new image sample and the stored template must meet or exceed the system's threshold before an image is accepted. The use of threshold and policies provide flexibility in the system (I/O Software, Jun 2002). The setting of the threshold, or error tolerance, of biometric systems is critical to their performance.

The overall performance of a biometric system is measured on how well it performs between the two kinds of variability among the acquired biometric templates:

- One-to-one (within-subject variability) - which sets a minimum False Reject Rate (FRR)
- One-to-many (between subject variability) - whose lower limit sets False Match or False Accept Rate (FAR)

Figure 4.5 shows the ideal biometric performance curve. The objective in setting a threshold is to have both errors (FRR and FAR) be low (I/O Software, Jun 2002). In practice, however, a low FRR usually means a high FAR and vice versa. Therefore, biometric systems designed for high-security applications, where concerns about unauthorized access are great, operate at a low FAR. As a result, the number of people who are falsely rejected is greater in these systems. Biometric systems designed for law enforcement applications operate at a high FAR. In these applications, the desire to catch a criminal outweighs the inconvenience of investigating a large number of falsely identified individuals (Encarta, Jun 2002).

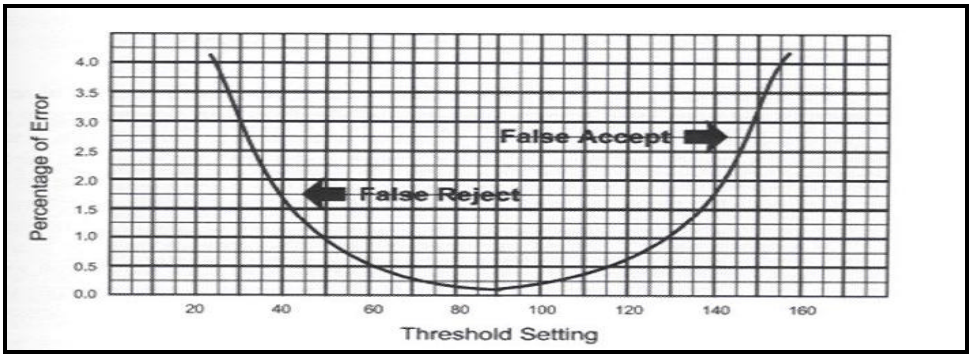


Figure 4.5. Ideal Performance Curve. (From: Ashbourn, p. 71).

2. Physiological Biometric Technologies

Physiological biometric techniques measure the physiological traits of a person. These physiological traits are stable physical characteristics, such as fingerprints, retina patterns, and iris patterns that remain essentially unaltered over a lifetime. Therefore, physiological biometric traits are ideal for application in smart cards for the proposed national ID card.

a. Iris Scan

The iris pattern of the eye is a biometric feature which exactly meets maximum between-subject variability (1:N) and minimal within subject variability (1:1) that is desired with biometric technologies (Jain, p. 103). The iris is the colorful part of the eye between the pupil and the white area of the eye. Based on clinical observations that every iris was unique and remained unchanged in clinical photographs (see Figure 4.6), ophthalmologists originated the idea that the iris of the eye could be used as a kind of "optical fingerprint" for personal identification (Polemi, p. 24).

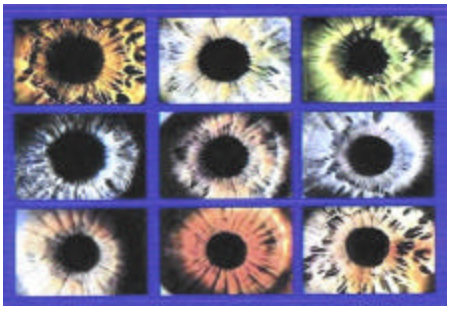


Figure 4.6. Iris Images. (From: Evangelista, 9 Feb 2001).

What makes the iris such a great tool for identification is that each iris consists of unique combination of contraction furrows, rings, crypts, freckles, vasculature, colorations, meshwork of connective tissue, fibers, a corona, processes, and other features (Polemi, p. 24). It has been mathematically proven that there are about 266 independent degrees of freedom in the iris among people to impart to it the same uniqueness as an individual's fingerprint (Jain, p. 103). According to IriScan, the leading iris technology company, the probability that two irises will create the same digital code is one in 10^{78} (Evangelista, 9 Feb 2001).

Iris scan technology uses a captured video image of the eye, encoding its unique features such as iris pattern and coloration. Iris scanners typically use video cameras and sophisticated targeting software to isolate and identify complex characteristic patterns that make up an individual's iris. Once the eye is located in the image, a series of concentric circular zones are produced that provide unique identifiable information about the iris (Ashbourn, p. 53). This data is extracted, and a digital code is created (see Figure 4.7).

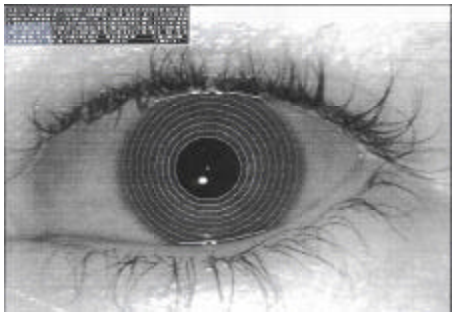


Figure 4.7. Iris Code. (From: Nanavati, p. 81).

An advantage of iris scanners (see Figure 4.8) over retina scanners is that they do not require the user to focus on a target because the patterns on the iris are located on the eye's surface. In fact, a video image of the eye can be taken from up to 36 inches away (Bioconsulting, 5 May 2001). This feature allows for the use of iris scanners at ATM machines. Sensar, Inc., a worldwide supplier of iris identification products for the banking industry, has a major contract with OKI Electric Industry, Ltd. who is the leading supplier of ATM's in Japan (Sensar, Jun 2002). Sensar has a similar agreement with NCR, the largest supplier of ATM's worldwide. Tables F.1 and G.1 list current iris scanning products and applications, respectively.

PC / Network Access *Physical Access*

Figure 4.8. Iris-Scan Devices. (From: Nanavati, p. 78).

Eye health does not significantly affect this technology. Iris scans can still be conducted on visually impaired persons as long as they have intact irises. In this situation, the iris can be captured and encoded with iris imaging products that have active iris capture, such as the ATM application mentioned previously. Since cataracts are a malady of the lens, which is located behind the iris, cataracts do not affect iris scanning in any way.

Countermeasures against deception have been developed, which include detecting a printed pattern on a contact lens by the using 2D Fourier domain artifacts of printing (Jain, p. 118).

Iris scanning strengths include the following:

- Technique is highly accurate (iris is more unique than a fingerprint) (Bioconsulting, 5 May 2001).
- Technique is highly resistant to false matching, and provides reliable identification as well as verification (Nanavati, p. 77).
- It is a stable measurement characteristic over a lifetime and is protected from the external environment (Polemi, p. 24).
- It is considered non-intrusive (Bioconsulting, 5 May 2001).
- It is easy to register an iris image at some distance from the subject without a physical contact (Polemi, p. 24).
- It is suitable for both logical and physical access control (Nanavati, p. 77).
- Process takes about 100 ms (Dygart, 1998)
- It is impossible to modify the iris without the risk of loss of vision.
- It is based on physiological response to light, providing a natural test (Polemi, p. 24).

Iris scanning weaknesses include the following:

- By comparison to other biometrics, it generates a relatively large template (256 bytes) (Bioconsulting, 5 May 2001).
- It has a propensity for false non-matching and failure of an individual's iris image from being acquired (~12%) (Bioconsulting, 5 May 2001).
- The core and key elements that have been developed for iris identification come from a single source and have been patented (Patent 5,291,590 by Dr. John Daugman) by IriScan, Inc. (Jain, p. 103). Its sole licensee is SENSAR (Bioconsulting, 5 May 2001).

- Although iris recognition offers probably the highest available accuracy and low intrusiveness, physical access models come at a relatively high price (Bioconsulting, 5 May 2001).

b. Retina Scan

The retinal blood vessels are a unique physical characteristic and provide a highly accurate means to verify an individual's identify. Retinal scans are performed by directing a low-intensity infrared light through the pupil to illuminate the interior of the eye and identify patterns in the capillaries on its back wall (see Figure 4.9) (Gomes, 27 Sep 2001). The image of the pattern of veins is reflected back to the camera. The sizes of veins, location of vein bifurcations, and capillary endings form a unique biometric pattern image that is used to differentiate people. The person undergoing the retinal scan must gaze into an eyepiece and focus on a designated spot for digital images of a fixed portion of the retina to be acquired. After the retina is scanned, special software creates a digital data image of the individual's unique pattern of retinal blood vessels. Once the image is processed and reduced from 16 kilobytes to 48 bytes, it is compared to a profile template that is stored in a centralized database or a smart card (Bioconsulting, 5 May 2001).

Figure 4.9. Pattern of Capillaries of the Retina. (From: Sullivan, 27 Sep 2001).

Since they offer one of the lowest FRR and a nearly 0% FAR, most retinal scanners (see Figure 4.10) are used in high-security access control applications where occasional false rejects are preferable to an impostor being able to defeat the system (Ashbourn, p. 56). Retina scanning systems are resistant to fraud since duplicate artificial eyes do not respond to light (Polemi, p. 24). While it would be hard to spoof retinal-based systems by constructing an accurate artificial model, an extracted eye could spoof

retina systems if it does not have a thermal test subsystem (Dysart, 1998). However, a person who had an eye transplant could spoof the system as long as the capillaries in the back of the eye were unaltered.

Figure 4.10. Retina Scanner. (From: Nanavati, p. 108).

Some medical research has recently shown that retinal patterns show critical variations in people with organ dysfunctional deceases (Polemi, p. 24). Cataracts can negatively affect the retinal image quality.

Though extremely accurate, retina scanners are highly intrusive, difficult to use, and typically cost $2,000 to $2,500 per unit (Raikow, 12 Mar 2001). There are only a limited number of retina-scanning products available on the market. EyeDentify owns U.S. and international patents, which protect the rights for exclusive use of retinal technology.

Retina scanning strengths include the following:

- It has a relative small template size, approximately 35 bytes.
- It has a high resistance to false matching (Bioconsulting, 5 May 2001).
- Retinas are a stable characteristic over lifetime, except in cases of certain degenerative retinal diseases or organ dysfunctional deceases (Polemi, p. 24).
- It provides relatively fast verification, typically in about 1.5 seconds (Ashbourn, p. 56).

Retina scanning weaknesses include the following:

- The amount of cooperation by the user that is required for a retinal scan make this technique unacceptable in many applications since refusal to cooperate is not apparent to the tester.
- Some users may find it difficult to use, typical user discomfort with eye-based technology.

- It is considered an intrusive technology.
- EyeDentify Inc. is the only current vendor for these products.
- This technology has not proven to carry out 1:N searching.
- Its products are expensive (Bioconsulting, 5 May 2001).

c. Fingerprint Scan

With its long history in law enforcement and government agencies worldwide, fingerprints are the most widely researched and understood biometric. The use of fingerprints as a biometric technique for identification traditionally has been employed by law enforcement agencies worldwide for over a century. In the past, fingerprint analysis and matching was conducted by hand and required significant time and effort. Today, Automated Fingerprint Identification Systems (AFIS) are used to automate the analysis and matching processes. They automatically analyze and match single fingerprints against large databases to find a proper match of all possible candidates (Dysart, 1998). The new techniques involved in acquiring a fingerprint image are very similar to the old-fashioned way of acquiring an ink fingerprint. A scan of the finger is taken using fingerprint scanning devices. They consist of a high-resolution digital camera behind a Plexiglas slate where the user presents a finger (Dygart, 1998). The camera creates data images that digitally contain the same distinctive ridge patterns that the ink process presents on paper. This data image is then compared to fingerprint templates of individuals that are stored in a storage device (database or smart card).

The geometric features and patterns of fingerprints are different for each person and tend to remain unchanged over a lifetime. The classification of a fingerprint is based on certain characteristics—arch, loop, and whorl (see Figure 4.11). The most distinctive characteristics are the minutiae, the forming patterns, the forks, or endings found in the friction ridges (see Figure 4.12), and the overall shape of the ridge pattern (Jain, p. 46). The fingerprint systems available for recognizing these characteristics use complex algorithms.

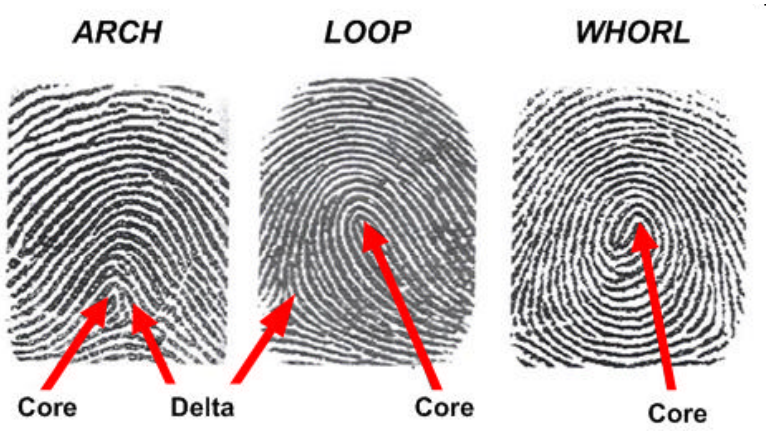


Figure 4.11. Fingerprint Classifications. (After: Jain p. 46).

Figure 4.12. Arch Pattern Fingerprint Minutiae. (After: Sullivan, 27 Sep 2001).

One disadvantage of fingerprint verification systems is that they are subjected to an imitation attack. Some systems are not capable of differentiating a fingerprint from a live user or a copied fingerprint. Prevention of these types of attacks have been addressed in some of the new systems by adding thermal sensors that detect subcutaneous blood vessels and reject a user if none are present (Dygart, 1998). A fingerprint reader can incorporate a heat sensor to gauge the presence of a real live finger versus a gelatin reproduction of the finger (Bhanbhani, 3 Jun 2002). Another disadvantage of using a fingerprint as a biometric is that the condition of fingers—finger surgery, injury, and deterioration due to heavy usage—might affect the performance of fingerprint verification systems.

In recent years, fingerprints have rallied significant support as the biometric technology that will probably be most widely used in the future. A GAO report stated that "fingerprinting may be the most viable option" among the various biometric methods investigated (Polemi, p. 23). Another study conducted by the CASCADE project claimed that fingerprint verification was the best technology to reduce passenger's clearance time through customs (Polemi, p. 23). In addition to general security and access control applications, fingerprint verifiers are installed at many military facilities, including the Pentagon and most government labs. Although fingerprint verification devices tend to reject over 3% of authorized users, the FAR is less than one in a million (I/O Software, Jun 2002).

Figure 4.13. Types of Fingerprint Products. (From: Nanavati, p. 46).

Due to its relatively high accuracy, low price, and minimal intrusiveness, fingerprint verification devices (see Figure 4.13) have been by far the most popular biometric for use in business and enterprise solutions. Individual fingerprint scanners typically cost between $100 and $150 (Raikow, 12 Mar 2001). Tables F.2 and G.2 list fingerprint products and applications, respectively.

Fingerprint scanning strengths include the following:

- A person's fingerprints are unique.
- Fingerprints are a stable physical characteristic throughout a person's life.
- There are a large number of huge databases already in existence.

- A large amount of research has already been conducted to develop and perfect fingerprint processing (image capture, template definition, matching, thresholds, etc.).
- It is considered non-intrusive.
- Equal Error Rate (EER) for fingerprint match algorithms can be very low (Bioconsulting, 5 May 2001).
- It is a proven technology, capable of high levels of accuracy.
- It can be employed in a wide range environments and applications (Nanavati, p. 58).
- It employs easy to use (ergonomic) devices (Nanavati, p. 59).
- The ability to enroll multiple fingers can increase system accuracy and flexibility (Nanavati, p. 59).

Fingerprint scanning weaknesses include the following:

- Certain ethnic and demographic groups have lower-quality fingerprints, therefore, some devices are unable to enroll some individuals in theses groups (Asian, elderly, manual laborers) (Nanavati, p. 59).
- There is performance deterioration (error increase) over time for users who work with their hands.
- It requires the deployment of specialized devices (Nanavati, p. 60).
- People with missing fingers cannot use fingerprint system. People with injured or swollen fingers might have a problem in being verified by these systems (Nanavati, p. 45).
- The template size is relatively large (~256 to 512 bytes per finger image) when compared to other biometric template sizes.
- Scanned images may become blurred due to injury, dirt on the scanning surface, or dirt on the finger.
- Processing requirements when performing a 1:N search of a huge database can be slow, unless many separate resources (matchers) are used together to process the match request (All other biometric techniques also suffer from this problem. Due to the sizes of current fingerprint databases, it is more prevalent with this biometric technique) (Bioconsulting, 5 May 2001).

d. Hand Geometry

The hand geometry biometric technique is based on the distinct characteristics of the hands. Hand characteristics measured include the external contour of the hand, internal lines of the hand, geometry of hand, length and size of fingers, palm

print, fingerprints, and the blood vessel pattern in the back of the hand. The same details are measured for finger geometry, a reduced form of the hand biometric technique, but they are conducted on only two fingers instead of an entire hand.

One form of the hand geometry technique employs hand geometry readers that use a digital camera to take an image of the top of the hand. To operate a hand geometry reader (see Figure 4.14), the user first enters a PIN number on the reader's keypad, and then positions a hand on a plate. The hand is lined up with five guide pegs on a platen that ensures that the hand will generally be located in the same position for every scan. Then a digital camera mounted above the plate, with the aid of a mirror, takes a picture of the top and side views of the hand (Dygart, 1998). The image is then transmitted into a computer for processing. Ninety characteristics in total are examined, including dimensions of the hand, length and width of the fingers, brightness of the skin, and shape of the knuckles (Gomes, 27 Sep 2001).

Contrary to the fingerprint, finger and hand geometry is not susceptible to incisions and chaps. Finger and hand geometry can still be influenced by major injuries of the fingers and the hand, and environmental conditions, such as dirt. Another technical problem is caused by the rotation of the hand when it is placed on the plate. The performance of these systems might be influenced if people wear big rings, have swollen fingers or no fingers. Paralyzed people or people with Parkinson's disease are not able to use this biometric method. (Polemi, p. 26)

Figure 4.14. Hand Geometry Reader. (From: Nanavati, p. 100).

Products that use palm print for identification or authentication are also available (see Figure 4.15). With these products, infrared scanners are used to take a digital image of the hand's palm. Each image is taken in less than a second. After registering the image data, the system compresses the biometric hand image and transmits it to a secure remote location via public/private key encryption. Then, a standard computer processor conducts an identity-match analysis against a database of pre-scanned hand templates, allowing a security system to grant access only to authorized individuals. This technology also employs measurement algorithms that tolerate some small changes in the palm over time.

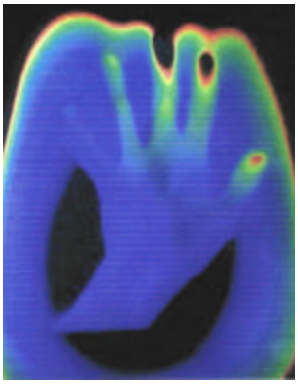


Figure 4.15. Hand Scan. (From: Evangelista, 21 Feb 2000).

Palm scanning technology is gaining popularity, and more and more deployments are being announced. This technology is mostly used in physical access control and in law and order areas. Currently, hand geometry systems are employed at over 3,500 locations, including the Colombian legislature, San Francisco International Airport, day care centers, welfare agencies, hospitals, and immigration facilities (Bioconsulting, 5 May 2001). The advantages of a palm print are similar to the benefits of a fingerprint in terms of reliability, although palm print readers take up more space. A survey following tests on various biometric devices concluded that hand geometry system was the user's overall favorite biometric when it was compared with fingerprint, signature, voiceprint, and retinal techniques (Polemi, p. 26). It was found, however, that cultural backgrounds do affect biometric device preferences. It has been found that,

although hand geometry is highly acceptable in most countries, people in Japan prefer not to place their palm where other people have (Polemi, p. 26).

Several factors can affect hand reader performance. Background environmental factors can influence hand reader performance. The hand image can be influenced by the direction of the sunlight as it relates to the platen. Temperatures can affect performance. Since below freezing temperatures and temperatures over 110 F cause problems for hand readers, most readers are designed to be used indoors in a controlled template environment (Polemi, p. 26).

Although hand geometry systems that are based on three dimensions (length, width, and thickness) are more secure, they can still be deceived by objects that accurately represent all three dimensions. These objects could include artificial models that reconstruct the bone structure of the individual or a detached limb (Polemi, p. 26). Like in fingerprinting, these attempts at evasion can be countered by the use of thermal sensors. Tables F.3 and G.3 list hand geometry applications and products, respectively.

Hand geometry strengths include the following:

- It develops a small sized template, about 9 bytes.
- Hand geometry systems are reasonably fast and provide short verification times.
- People tend to view it as non-intrusive.
- It provides satisfactory one-to-one match accuracy (FRR/FAR) for middle security applications (Bioconsulting, 5 May 2001).
- Some hand geometry readers have the ability to operate in challenging environmental conditions (Nanavati, p. 103).
- It is an established and reliable core technology.
- Hand geometry is a relative stable physiological characteristic.
- It provides a balanced combination of convenience and deterrence (Nanavati, p. 104).

Hand geometry weaknesses include the following:

- It provides inherently limited accuracy for high-level security applications.
- Its form factor (reader size and shape) limits the scope of potential applications (Nanavati, p. 105).

- Hand geometry readers are expensive.
- It has no proven open search (1:N) capability.
- Readers are relatively large and can be easily damaged (Bioconsulting, 5 May 2001).

e. Facial Recognition

Facial recognition is one of the fastest growing sectors of the biometrics industry. It is perhaps the most active area for deployments and the one that has been receiving most of the headlines, particularly in the post-9-11 era, when airport security and public safety are of paramount importance. Its appeal lies in the fact that identification of an individual could be conducted at a distance without having the individual physically interact with the system. Its employment efforts have also been stimulated by the fast rise in multimedia video technology that is placing more cameras in public areas, in front of computers, and in the workplace. However, the technology is still considered to be in its infancy, and additional testing for full-scale deployment is required. Nevertheless, specific applications, such as monitoring airport lounges and sporting events for suspected terrorists, and screening driver license or welfare databases for duplicates are being employed.

The theory behind facial-recognition technology is that facial characteristics are unique and can be used to reveal an individual's identity. This technology uses computer software to scan a picture captured from video from surveillance cameras. Then, the system imports the image and encodes measurements between distinctive facial features, a process called triangulation, using neural network methodologies and algorithms. Face-recognition technologies use a variety of techniques to identify unique or unusual facial features and the distances between them (see Figure 4.16).

Figure 4.16. Facial Landmarks. (From: Blackburn, 10 Aug 2001).

Details of the face that are used include the distance between the eyes, the hairline, the outline of the face, angle of the chin, size of nose, shape of eyes, shape of chin, shape of eyebrows, color of the skin and shape of mouth, all relative to other locations on the face (Polemi, p. 25). Once an image is captured and stored in a database or smart card as a template, it is used to compare against other facial biometric templates that exist in large databases (Gomes, 27 Sep 2001).

The latest versions of facial recognition software can be used in conjunction with closed circuit television surveillance systems to provide additional help in the fight against crime and terrorism. While the resulting collection of facial data does not have the uniqueness of other biometrics such as DNA, iris, fingerprint, and retina scans, it can still be useful as a valuable non-intrusive way of monitoring for suspected terrorists, provided the individual pre-exists in a database. By comparing faces in a crowd with a database of known criminals and suspected terrorist, law enforcement can pinpoint likely suspects and take action when appropriate.

Facial-recognition technologies have some weaknesses that have prevented agencies from embracing the technology. Though non-intrusive and low cost, facial recognition systems offer relatively limited accuracy and may require substantial processing power in a commercial IT environment (Raikow, 12 Mar 2001). Facial recognition systems have difficulty identifying identical twins as different persons. Some facial recognition systems are unable to cope with angles or facial expressions, which are a little different from those used during the enrollment process. Some systems are not able to analyze people with imposed physical characteristics such as a beard, styled hair, disguises, or with certain facial expressions. Templates are also required to be updated periodically because changes occur in the facial skeleton during the human aging process. Algorithms are still being trained to accommodate for factors such as aging, image resolution, and lighting variances in different photos (Ellis, 15 Sep 2000).

With some existing facial recognition systems, certain restrictions are imposed on the user. The user must look straight into the camera with certain lighting available in order for the system to analyze and identify the person. However, various new graph-matching techniques are being developed that enhance the quality of picture, thus decreasing these constraints.

Visionics FaceIT System (see Figure 4.17) and Viisage Technology‘s FaceFINDER (see Figure 4.18) are two of the most popular systems that are available right now. Visionics' FaceIt system measures approximately 80 facial characteristics of a person and compares them with templates that are stored in a central database. The system needs to see 15 to 20 of these characteristics to make a match, so obstructions such as hair blocking the face can impede the system. This weakness can be eliminated by using the technology at passenger check-in or at different checkpoints where personnel are forced to face a camera without obstructions (Stikeman, Dec 2001).

Facial recognition technology is improving; and its algorithms are evolving the capability to match faces regardless of age, facial hair and other alterations. The use of extra cameras can increase accuracy, and provide the ability to provide combine multiple views to create three-dimensional (3D) images (Stikeman, Dec 2001).

Tables F.4 and G.4 list facial recognition scanning products and applications, respectively.

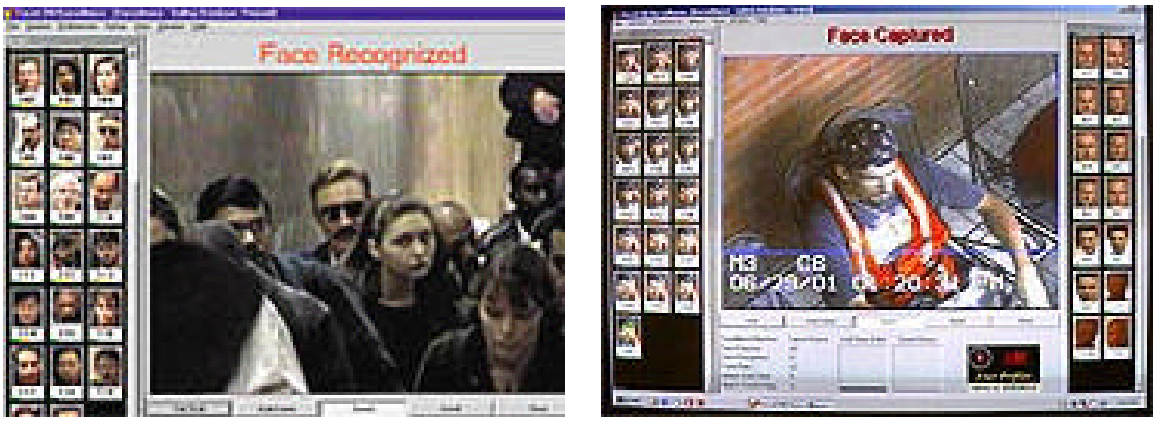


Figure 4.17. Visionics' FaceIT System. (From: Cass, Jan 2002).

Figure 4.18. Viisage Technology's FaceFINDER System. (From: Cass, Jan 2002).

The strengths of facial-recognition include:

- Since facial-recognition technologies are software-based, they can be deployed without additional proprietary hardware. In most cases, it has the ability to leverage existing image acquisition equipment, such as CCTV cameras or standard video cameras that are already installed.

- Facial-recognition technology is one of the only biometric techniques available that allows use without physical contact, user involvement, or awareness.
- Facial-recognition technologies allow the enrollment of static images (pictures).
- It is non-intrusive (Nanavati, p. 73).

The weaknesses of facial-recognition include:

- Matching accuracy can be affected by the acquisition environment (lighting, camera position, acquisition angle, background composition).
- Matching accuracy can be reduced by the changes in physiological characteristics (hairstyle, makeup, facial hair, addition or removal of eyeglasses, addition of hats or scarves).
- There could be a perception of potential privacy abuse due to non-cooperative enrollment and identification (Nanavati, p. 74).
- It can have difficulty in distinguishing identical twins.
- When compared to other biometrics, Equal Error Rate (EER) for facial algorithms can be much higher (Bioconsulting, 5 May 2001).

3. Behavioral Biometric Technologies

A behavioral characteristic, like one's voice, signature, or keystroke dynamics, is influenced by controllable behavioral actions as well as less controllable psychological factors. Since behavioral characteristics can change over time, the enrolled biometric reference template is required to be periodically updated (I/O Software, Jun 2002). For this reason, these biometric techniques have limited applications in the war against terror.

a. Voice Recognition

A person can be identified by the various characteristics of the sounds, vocals, and phonetics the person makes as he or she speaks. A person's vocal characteristics such as mouth, nasal cavities, and vocal tract produce speech patterns that are relatively "unique" and different for other people. Although humans can use these characteristics naturally for identifying someone, a complex algorithm is required for a computer system to analyze the voice characteristics (see Figure 4.19). Speech recognition technologies use voice recordings to create voiceprints based on inflection and the distinctive highs and lows in a person's speech (Gomes, 27 Sep 2001).

Figure 4.19. Voiceprint Characteristics. (From: Sullivan, 27 Sep 2001).

With voice recognition systems, a person speaks into a microphone or over a telephone attached to the system. The system then analyzes the voice characteristics of the voice sample. The system typically uses Fourier-based methods to extract the biometric features and create a template of the "voiceprint." Finally, the system compares the characteristics of the newly produced template with the voice characteristics of a prerecorded template.

Since they require only standard microphones or modems built into most modern PCs, voice-recognition systems are extremely cheap. They are non-intrusive and can be used over a telephone or other remote voice connection. They, however, offer relatively poor accuracy, and are often highly vulnerable to background noise and other environmental factors (Raikow, 12 Mar 2001). The use of Time Encoded Speech (TES), a form of waveform coding, combined with the use of artificial neural network architectures, has allowed its use in high background noise environments (Polemi, p. 28). New systems are based on a technology called Time Encoded Signal Processing and Recognition (TESPAR), which is a simplified digital language for coding speech. It provides a simple way of generating a template that defines any sound. Its method differs from the classical Fourier analysis of previous systems. It works by analyzing snapshots of a sound wave image template against time without calculating frequencies (Polemi, p. 27).

There are several problems associated with this biometric technique. Voice verification is not as accurate as other biometric techniques. Some systems have

tedious enrollment procedures. Illness, fatigue, and stress can also cause problems in voice verification. Women generate more complex voice frequencies, which make it harder to identify them. People affected by alcohol, by dental anesthesia, by oral obstruction also will have difficulty being verified by voice verification systems (Polemi, p. 28). An individual's voice can change over his lifetime; therefore, it requires enrolled templates to be updated periodically. There is also fear that, as digital recording equipment evolves and becomes more sophisticated, accurate reproduction of a person's voice will be possible in the not to distant future (Polemi, p. 28).

Another concern about this biometric approach is impersonations. However, since these devices focus on different characteristics of speech than people do, it is not considered a problem. Although an impersonation may sound similar to human ears, it is not when analyzed by voice analyzers. Duplication of voice using a tape recorder is more of a major threat to these systems. As digital recording systems are enhanced and become more advanced, some systems will not be mathematically capable of differentiating between real and prerecorded voices.

Presently, systems developers are combining voice verification with other forms of security and surveillance technologies (Polemi, p. 28). It is currently being deployed in radio or telephone communication surveillance to identity individuals, such as suspected terrorists and their associates. Tables F.5 and G.5 list voice recognition products and applications, respectively.

The strengths of voice verification include:

- It is easy to use.
- It is considered non-intrusive (Bioconsulting, 5 May 2001).
- One can leverage existing telephony infrastructure.
- It can be effectively layered with speech recognition and verbal account authentication.
- It is relatively resistant to imposters.
- It generally does not have the negative perceptions that are associated with other biometrics (Polemi, pp. 94 and 95).

The weaknesses of voice verification include:

- As digital recording media becomes more advanced, voice authentication/recognition becomes more susceptible to replay attacks than other biometrics.
- Its accuracy is challenged by ambient noise and low quality capture devices.
- People are usually unaccustomed to speaking to their computers.
- It has a large template size (typically 250 to 1000 bytes) (Polemi, pp. 95 and 96).
- A person's voice can vary with their mood (anger, depression, excitement, etc.) or health (cold, flu, etc.) (Bioconsulting, 5 May 2001).

b. Handwriting/Signature Recognition

Handwriting/Signature Recognition is based on an individual's reflex action that is not influenced by deliberate muscular control. Writing characteristics such as rhythms, pen pressure, successive touches of the writing surface, measurements of spacing, number of contracts on the surface, duration the pen touches the tablet, total time of writing a signature, turning point, number of horizontal turning points, loops, slopes, velocity, and acceleration tend to be unique for each individual. This method uses sensors to detect dynamic rhythms, speed, and pressure exerted by the hand when an individual is writing. The static shape of the completed signature is also analyzed (Gomes, 27 Sep 2001) (see Figure 4.20).

There are two methods in use to identify a person based on signatures: static and dynamic. The static method compares already written signatures with a signature from a reference source. Static signature capture is becoming quite popular as a replacement for pen and paper signing in bankcard, PC, and delivery-service applications, such as those used by package delivery services.

The second method examines the dynamics of the signature when it is written down. Since it is more difficult to imitate a signature that is controlled dynamically, most of the commercially available signature-verification systems and those under development are based on dynamic signature verification (Nanavati, p. 125). The development and use of artificial neural networks have made these systems more accurate and cheaper.

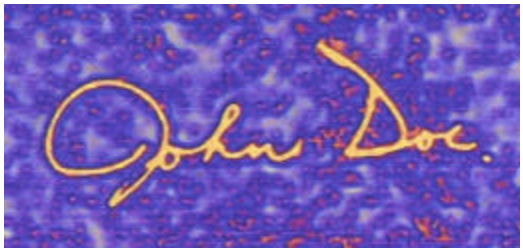


Figure 4.20. Handwriting Recognition Image. (From: Evangelista, 21 Feb 2000).

Signature verification devices use wired pens, pressure-sensitive tablets, or a combination of both. Devices using wired pens are less expensive and take up less room but are potentially less durable. Dynamic signature-verification systems use sequential methods to divide the signature into independent events, and examine each piece separately (I/O Software, Jun 2002). Multiple enrollments are often required for some systems (Nanavati, p. 126). At the time of verification, the user is asked to sign. The system compares various aspects of its signature on a hierarchical manner. If a good match is not found between the signatures characteristics of the new template and the stored template, the new template is rejected.

Since signature is a familiar way in identifying individuals, hand written signature verification systems can be highly acceptable. In a survey performed by a branch of a UK Post Office, a signature verification system was preferred over the fingerprint system (Polemi, p. 29).

There are still some challenges with the use of signature-verification technologies. Some systems have had difficulties with people that change their signature often or radically. Other systems cannot distinguish pen pressure from palm pressure. Signature dynamics can be affected if a person has an injury, illness, or is under the influence of drugs or alcohol. People with Parkinson's disease are not able to use these systems. This technology also cannot be used in countries with low literacy rates. To-date, the financial community has been slow to adopt automated signature verification methods for credit cards and check applications because signatures can still be too easily forged. This keeps signature verification from being integrated into high-level security

applications. However, electronic signature verification is gaining ground in retail and e-commerce applications (Polemi, p. 29).

There are about ten products commercially available, and about the same number are under development. Applications in the war against terror could include identifying origins of terrorist-related correspondence. An example of this application was the Israeli analysis of the paper trail of the arms shipment to the Palestinian Authority and their request for funds for suicide bombings. Tables F.6 and G.6 display signature verification applications and products, respectively.

The strengths of signature verification include:

- It is resistant to imposters.
- It leverages existing processes.
- It is perceived as non-invasive.
- Users can change signatures (Nanavati, p. 123).

The weaknesses of signature verification include:

- Inconsistent signatures can lead to increased error rates.
- Some users are unaccustomed to signing on tablets.
- It has limited applications (Nanavati, p. 123).

c. Keystroke Recognition

The theory behind keystroke analysis is that every individual has his unique pattern or rhythm of typing. The combination of typing speed, the duration of a keystroke, time lapses between keystrokes, typing error frequency, forced keystrokes, and time lapses when two keys are stroked simultaneously are relatively unique per individual (Polemi, p. 30). These characteristic details of a user's typing "signature" can be used for identification. During the enrolment phase, the average and deviation of these details are calculated and stored in a template for use in the future. Identification of individuals becomes easier if the analyzed individuals are trained typists.

The Keystroke Analysis software analyzes an individual's keystroke dynamics or typing rhythms by monitoring the user's keyboard input 1,000 times a second (I/O Software, Jun 2002). One of the advantages of this technique is that neither enrollment nor verification detracts from the regular workflow (I/O Software, Jun 2002).

Two kinds of systems have been developed. One uses a static verification technique while the other uses a dynamic verification technique. The static technique uses a neural network approach for pattern recognition to analyze the way a username or password is typed. Dynamic approach uses statistics to verify the person continuously with any arbitrary text input. (Polemi, p. 30)

Despite its appeal in some sectors, efforts to commercialize the technology have failed. Due to the infancy of the technology and the possible variations of keystrokes a user may have, this method of authentication or verification should only be offered as supplement to some secure authentication mechanism and not to be used independently. Hand injuries, distractions, and fatigue can affect the accuracy and performance of this method (Polemi, p. 30). Several universities and research laboratories are studying keystroke dynamics, and are developing identification, or authentication systems using this technology (I/O Software, Jun 2002). Companies and laboratories developing products that use keystroke dynamics are listed on Table F.7.

Applications for this biometric technique, with some modifications, in the war against terror could include pre-deployment at cyber-cafes known to be frequented by suspected terrorists to aid in monitoring an individual's use of the Internet.

The strengths of keystroke recognition include:

- It leverages existing hardware.
- It leverages common authentication process.
- It can enroll and verify users with little effort (Nanavati, p. 133).
- Individuals can change their usernames and passwords but their keystroke behavior remains relatively the same.

The weaknesses of keystroke recognition include:

- It is a young and unproven technology.
- It does not increase user convenience.
- It retains many flaws of password-based systems (Nanavati, p. 134).
- It requires an expensive system (system uses neurological methods and dedicated terminals) (Polemi, p. 30).

d. Gait Recognition

While automated face recognition receives the most attention of non-intrusive biometric technologies, Defense Advanced Research Projects Agency (DARPA) is also funding efforts at a handful of universities to identify people through their body language (Cameron, 23 Apr 2002). There is research interest on recognizing people by their gait. The theory is that each person creates his or her own distinct "gait signature." In the same way that each person has a unique fingerprint, iris, retina, or signature, each person also has a unique walk or gait. Distinguishing one person's gait from another's is something some researchers believe they will be able to do reliably enough in the not too distant future to aid in "surveillance situations," especially when someone's face is not visible (Ellis, 5 Sep 2000). Since a person's gait is characterized by hundreds of kinetic parameters, it is believed that a gait is distinguishable and hard to "fake" or hide. People can hide or disguise their faces but they cannot change the way they walk and still look "normal." The reason for this new interest is that unlike faces and irises, a gait can be analyzed from a great distance even with low-resolution cameras (surveillance video, home video).

The DARPA effort on Human ID at a distance is a sub-program of the gait research. Although DARPA's interest is primarily in potential military and security applications, other researchers envision a broad range of uses, including:

- Automatic person identification in video sequences
- Identify the shopping patterns of different demographics
- Recognize shoppers who return within half-hour – then forget them to protect their anonymity
- Use with every-day computer interfaces (Sciencenet, Dec 1999)

As with many applications of pattern recognition, the studies being conducted on gait recognition concern statistical recognition and model-based recognition. Statistical recognition deploys principal components analysis for data compression, canonical analysis (see Figure 5.21) for improved recognition, processing of threshold-image, and optical flow data. Relationship to the mechanics of a gait has been achieved by a new approach that uses statistical moments computed for moving objects, called "velocity movements." Database techniques extract particular features of

a person's gait such as the shape and angular velocity of a limb or the length of a joint (Sciencenet, Dec 1999). Recognition can also be derived from the motion of a subject's silhouette mathematical characteristic root, called an eigenvalue (see Figure 5.22). Statistical methods similar to automatic face recognition can also be used to recognize people by their gait (ISIS, 9 Jan 2001).

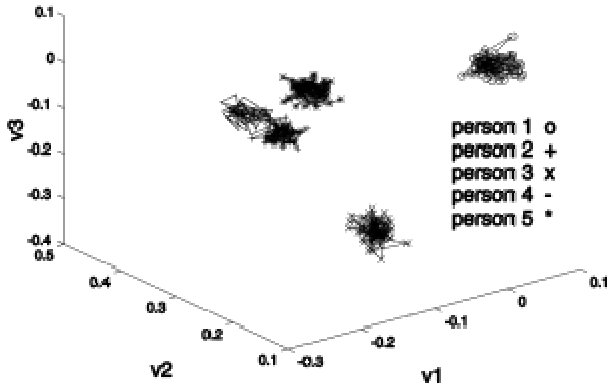


Figure 4.21. Canonical Space Trajectories of Five Subjects. (From: Jain, p. 242).

Figure 4.22. Eigenvalue of a Silhouette. (From: ISIS, 9 Jan 2001).

Model-based recognition considers human motion to be that of a moving pendulum. This method has allowed development of a gait signature based on the variation in inclination of the human thigh (see Figure 4.23). This method uses the pendulum-like motion of the leg joints extracted from an image sequence to analyze a gait (Sciencenet, Dec 1999). The gait is modeled as Simple Harmonic Motion (SHM)

and the indication to identity is the difference between perceived motion and that of pure SHM.

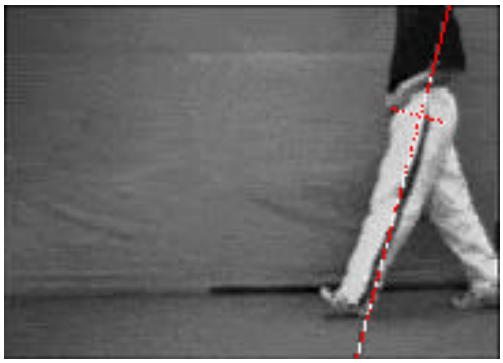


Figure 4.23. Example of Simple Harmonic Motion Analysis. (From: ISIS, 9 Jan 2001).

Prototypes that use gait recognition techniques have already been created that can filter out noise from a video image and recognize a person walking past a moving camera even in windy or cloudy conditions (Ellis, 15 Sep 2000). Applications of gait recognition technologies include bulk surveillance in public areas or in the battlefield, if gait templates exist on file in a database (Ellis, 15 Sep 2000). Future research involving this technology should include the ability to identify individuals from a distance using aerial surveillance (Predator).

The strengths of gait recognition include:

- Accuracy is about 90-95% (Cameron, 23 Apr 2002).
- Each person tends to have a distinct gait.
- General perception as non-intrusive, passive surveillance.
- Provides vehicle for testing motion-based evidence gathering techniques (ISIS, 9 Jan 2001).

The weaknesses of gait recognition include:

- Technology is in its infancy.
- Database technique is poor at ignoring flapping clothing when analyzing the gait of a person.
- Currently, all database images are two-dimensional and depend greatly on the angle of the camera (ISIS, 9 Jan 2001).
- When a system tries to compare two sequences of the same person, taken at a different angle, it is far less effective. This weakness can be addressed

with computer-graphics techniques that re-render images at new angles. (Cameron, 23 Apr 2002)

4. Other Emerging Biometric Technologies

Lack of standards or independent testing, as well as high deployment costs, are the weak points of the following technologies:

a. DNA

All human cells, except for the red corpuscles, contain a core of genetic information, which is unique for every individual (Polemi, p. 30). This core of genetic information is called DNA (Dysart, 1998). The genetic information that is encoded in DNA may be the ultimate source of identification. Identification or verification using DNA (see Figure 4.24) is regularly used in forensic laboratories. The amount of material needed for such an analysis is very small; e.g., one hair or a drop of saliva is sufficient. The major advantage with this biometric technique is that a DNA print is the same for every cell or tissues of the body (Polemi, p. 30).

The basic concerns against this technique are the ethical and practical acceptability from the user. There is a strong resistance against the use of DNA for identification or authentication in common applications. This resistance lies in the fact that human cells need to be taken from the human body. There is also the perception of the potential use and misuse of additional information contained in the DNA.

The major area of application for DNA technologies will continue to be criminal justice. This method is widely used in forensics to identify criminals and unknown corpses (Polemi, p. 31). Its application in the war on terror would remain the same, verifying the identities of dead and captured terrorists.

One of the major disadvantages of DNA pattern recognition is that it is a laboratory procedure that requires the isolation of the DNA, processing, transfer of DNA to nylon, and probing, and thus is an expensive process that requires time to perform before results of identification are available (Polemi, p. 31).

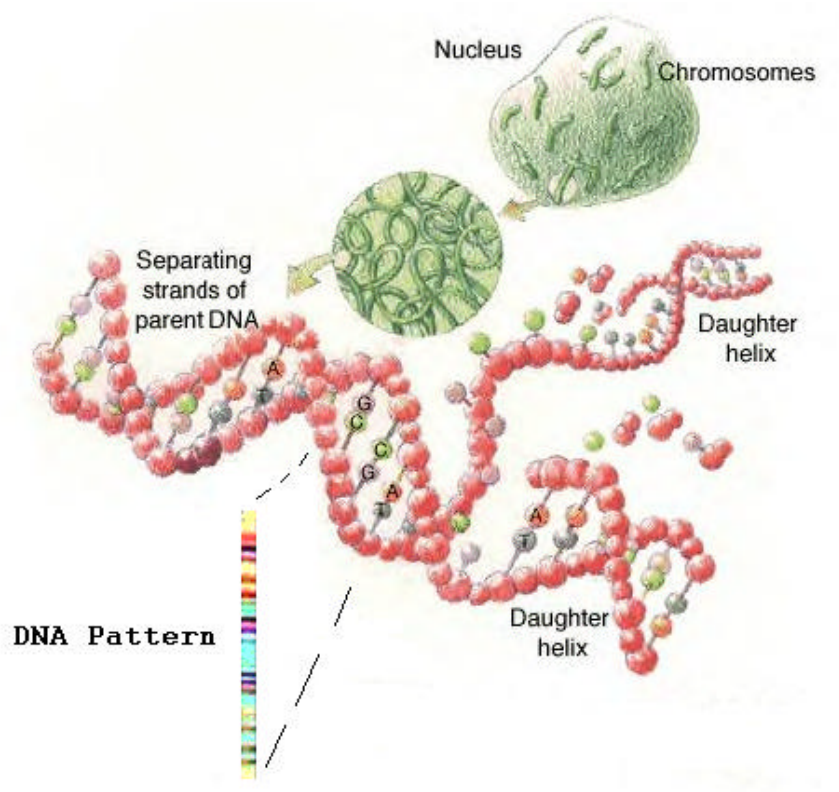


Figure 4.24. DNA and DNA Pattern. (After: DOE Human Genome Project, 2002).

b. Vein Pattern Recognition

Vein pattern recognition is an idea for identification that is being considered by some researchers. In this technique, the veins of the back of the hand and wrist (see Figure 4.25.) are scanned while the user grips a bar of a reading device (Ashbourn, p. 63). Prototypes of various vein recognition systems have already been developed that obtain two-dimensional scan images of the vein patterns of the back of the hand and develop templates using numerous vein pattern matching algorithms (Polemi, p. 26).

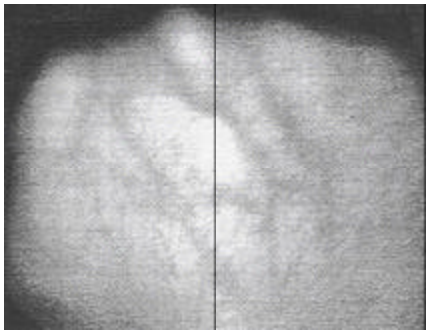


Figure 4.25. Vein Pattern. (From: Jain, p. 7).

The British Technology Group (U.K.) is one research group, which is working on this technology by developing their Veincheck Systems.

The strengths of vein-pattern recognition include:

- It is relatively tamper-proof .
- It is not easily damaged by minor abrasions (Ashbourn, p. 63).

The weaknesses of vein-pattern recognition include:

- There is low interest in the technology (Ashbourn, p. 63).
- Its form factor (Reader size and shape) limits the scope of potential applications.
- General perception is that it is intrusive (Polemi, p. 26).

c. Ear Recognition

Ear Recognition technologies allow the identification of an individual by the shape of the ear. The theory behind this technique is that each person's ear has unique characteristics for a given individual—a distinct bone structure and shape of the outer ear and ear lobe (Gomes, 27 Sep 2001). With the help of a video camera, an image is taken of the ear, which is then analyzed and used for further identification or authentication. Currently there are to types of methods that have been developed to analyze the ear. One method (see Figure 4.26.) uses the anthropometric measurements and locations of ear characteristics—[1] Helix Rim, [2] Lobule, [3] Antihelix, [4] Concha, [5] Tragus, [6] Antitragus, [7] Crus of Helix, [8] Triangular Fossa, and [9] Incisure Intertragica—to develop an ear template. The other method (see Figure 4.27) develops an ear biometric graph model by first tracing the features of the ear,

constructing a Voronoi diagram, and creating a Neighbor Graph that is used to form the ear template.

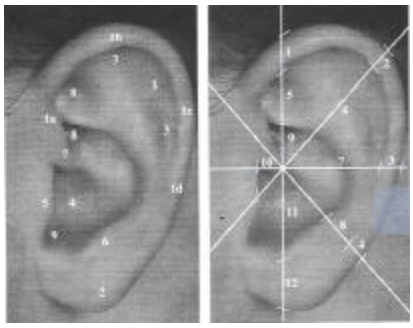


Figure 4.26. Ear Shape Biometrics. (From: Jain, p. 277).

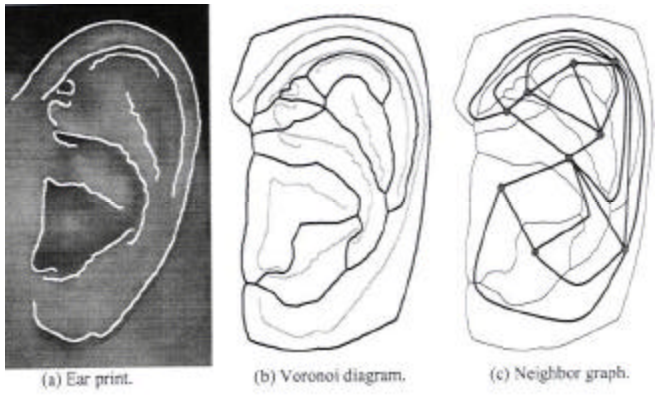


Figure 4.27. Stages of Building the Ear Biometric Graph Model (From Jain, p. 279).

This technique has already been used by law enforcement to identify criminals. Currently few products available apply ear pattern recognition. One of these, created by ART Techniques (U.S.) and called Optophone, was built into the ear part of a telephone (Polemi, p. 31).

d. Odor/Scent Identification

This olfactory biometric technology uses sensors that recognize the unique chemical patterns of human body odor to determine a person's identity (Gomes, 27 Sep 2001). While humans and animals use body odor as a basic qualitative biometric, using it as an accurate representation for identification purposes may seem a little strange, but there has been much research in this area. The theory of this technique is that 30 chemicals substances a body emits, called "rolatiles," make up a person's distinctive

smell (Dysart, 1998). A system or device using this technique uses a number of chemical receptors and sensors that generate a difference in voltage in case a particular substance is present. With the help of neural networks, it is possible to disentangle specific scent patterns. The differences in voltages are used to differentiate the different compounds that make up a person's scent. This method is under development and its applications are limited. A system called "Scentinel" was being developed in 1997 using this biometric technique by Mastiff Electronics (Polemi, p. 31). This biometric technique has received very little interest for deployment in real-world applications (Dysart, 1998).

e. Thermal Facial Scan

Thermal facial-scan (see Figure 4.28) is a biometric technology that was first developed in the mid-90s (Nanavati, p. 113). This technique measures the infrared patterns caused by the distinct flow of blood under the surface of the skin of the face.

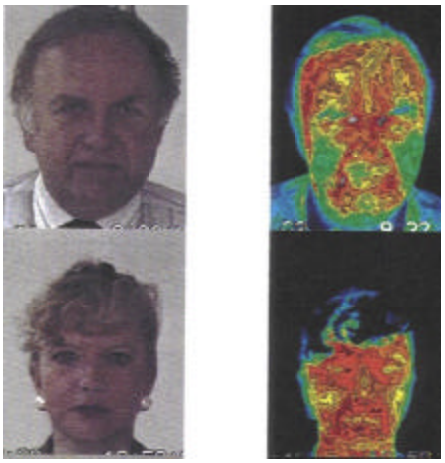


Figure 4.28. Thermal Facial-Scans. (From: Jain, p. 195).

As a biometric identification technique, it has been shown to be highly distinctive with a stated accuracy of 85 to 98 percent (Jain, p. 212). In addition to identification, thermal face-scans have been tested to detect lies (see Figure 4.29) almost as good as polygraph machines and could identify people under stress that might be undertaking a hostile action (DeNoon, 25 Jun 2002). Thus, this technology might be useful in interrogations or in monitoring crowds.

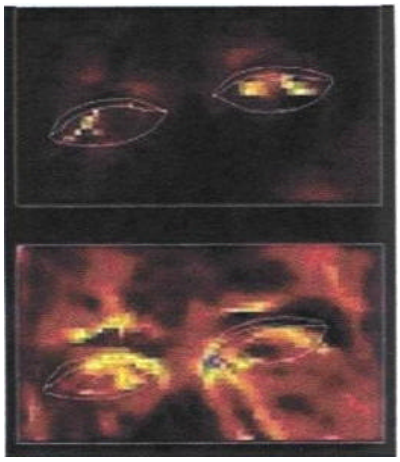


Figure 4.29. Non-Intrusive Lie Detector. (From: DeNoon, 25 Jun 2002).

f. Subcutaneous Hand-Scan

Subcutaneous hand-scan analyses the palm's tissue structure below the surface of the skin. The outlook for this technique is reasonably strong. Prototypes have already been built and have attracted some interest. (Nanavati, p. 113)

g. Sweat Pore Analysis

In 1823, Czech Jan Evangelista Purkinje, while studying sweat glands, observed that precise patterns of grooves and ridges resulting from the sweat pores of the skin seemed to be unique and believed that the distribution of the pores in the area of the finger was distinct for a given person (Ashbourn, p. 5). Based on this theory, sweat pores analyzers have been developed which analyze the sweat pores on the tip of the finger. When the finger is placed on the sensor of the sweat pore analyzer, the analyzer's software records the pores as stars and stores their position relative to the area of the finger (Polemi, p. 31). Interest in this biometric technique remains low.

h. Nail Bed Identification

Nail bed Identification techniques are currently being studied. This technique analyses the vertical ridges beneath the human fingernail (Nanavati, p. 113). There appears to be no real future for this technique, however.

C. SCANNERS AND SNIFFERS

To improve surveillance capabilities at airports, ports, and our borders, new scanning and "sniffing" security equipment is already being employed to supplement traditional metal detectors and screening procedures.

1. Scanners

a. Explosive Detection System (EDS)

Prior to 9-11, carry-on baggage typically went through an X-ray scanner. Today, improved scanning devices, similar to Invision's computer tomography (CT) machines (see Figure 4.30), are required and are being employed to do a better job at detecting weapons. CT scanners use an x-ray mechanism that revolves slowly around baggage to obtain image data or tomogram (see Figure 4.31). The scanner is able to determine the mass and density of individual objects and alert operators if an object's mass and density falls within the range of a dangerous material (Tyson, Jun 2002).

CTX 5500 DS CTX 9000 DSi

Figure 4.30. Explosive Detection Systems from Invision Technologies. (From: Invision-tech.com, 2002).

The major problem with these systems is that they cost over $1 million each, occupy large areas, and the suppliers cannot meet the required demands made by the new Transportation Security Agency (TSA). In the meantime, to meet the new safety guidelines, many airports are using the more readily available and less expensive Explosive Trace Detectors (ETDs). Due to the short supply of EDS machines, more than 740 ETDs are now being used in conjunction with metal detectors and x-ray machines at airport security checkpoints (Orenstien, Nov 2001).

Figure 4.31. CT Mechanism and Tomogram. (From: Tyson, Jun 2002).

b. Body Scanners

The FAA has tested a low-power X-ray machines, such as BodySearch (see Figure 4.32) and Rapidscan's Secure 1000, to allow the operators to detect any hidden drugs, weapons, or explosives (CNN.com, 21 Aug 2000 and Masterson, 3 Apr 2002).

Figure 4.32. BodySearch Technology. (From: CNN.com, 21 Aug 2000 and NewsMax.com, 9 Mar 2000).

The systems reflect X-rays, which penetrate only a few millimeters below the skin, producing images that can be analyzed by the operator. Similar detection devices are already deployed at some international airports, prisons, and customs checkpoints. In 2000, customs officials had already deployed these body scanners at JFK Airport in New York, Miami International, Chicago's O'Hare Airport, Atlanta's Hartsdale Airport, Houston Intercontinental, and Los Angeles Airport (NewsMax.com, 9 Mar 2002). Before Sept. 11, the FAA believed the privacy issues were difficult to overcome. Since 9-11, with the public demanding more security, more deployments at major airports are likely.

c. Cargo, Truck and Vehicle Scanners

New scanning technologies have been developed to aid in the inspection of cargo, trucks, and vehicles. With significant financial support from the U.S. Government, Ancore Corporation has developed Pulsed Fast Neutron Analysis (PFNA) and Thermal Neutron Analysis (TNA) that can aid in inspecting cargo at airports and seaports as well as inspecting trucks and vehicles at weigh stations and border crossings (Gozani, 12 Mar 2002). TNA technology (Figure 4.33) uses a small neutron source or an electronic neutron generator to produce neutrons that in turn are used to detect bulk quantities of explosive and drugs concealed in trucks or cargo containers (Brown, 19 Feb 2002).

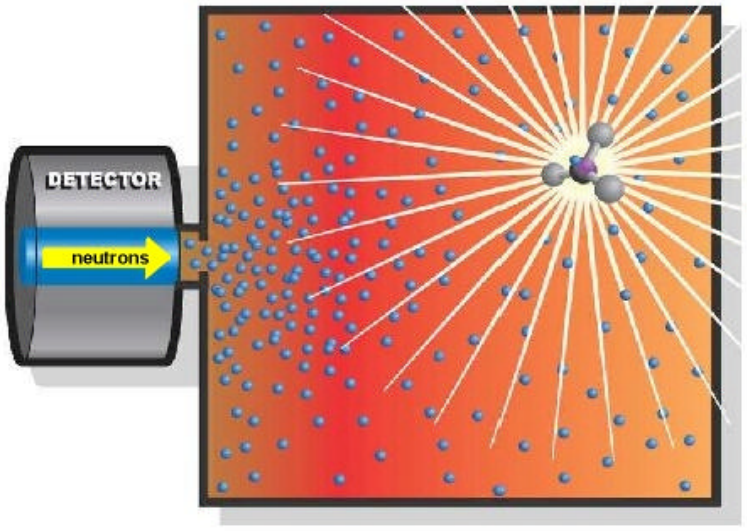


Figure 4.33. TNA Material-Specific Inspection. (From: Brown, 19 Feb 2002).

The neutrons are used to interact with the inspected materials. TNA detectors then measure the signals resulting from the interactions. Each signal is unique to a given element. According to Dr. Tsahi Gozani of Ancore Corporation, "TNA devices can be readily augmented to detect passively and actively nuclear materials (Gozani, 12 Mar 2002)."

Currently, PFNA technology is the only automated, non-intrusive, material-sensitive technology available to inspect large shipping containers, cargo containers, and trucks (Gozani, 12 Mar 2002). PFNA (Figure 4.34) measures the elemental contents within small volumes, called voxels, of an inspected object.

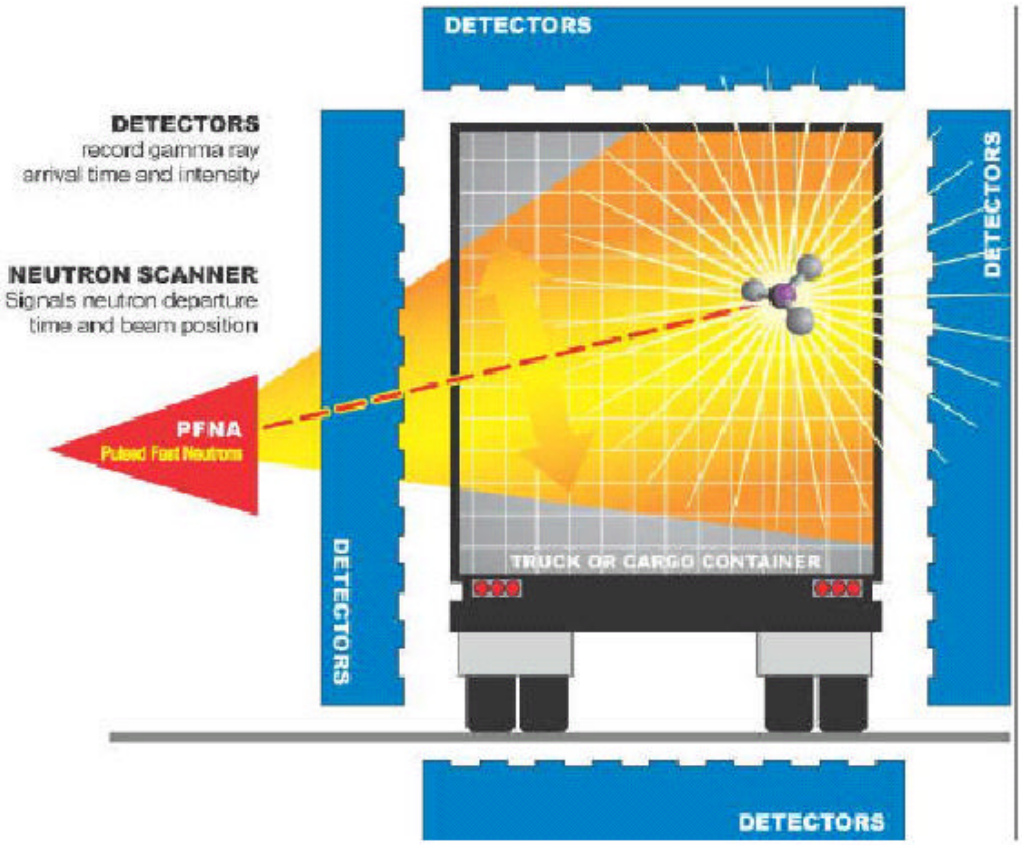


Figure 4.34. PFNA Inspection Process. (From: Brown, 19 Feb 2002).

Inspected objects are scanned by the system using short pulses of fast neutrons. The bombardment of the object and its contents by fast neutrons results in the

emission of gamma rays. Gamma detectors, located strategically around the inspected object, collect the gamma rays, which were omitted. Then an electronic data acquisition system processes the signal and routes the elemental signal data to the system's computer, which further processes the data and produces elemental images of what elements are present in the container (Brown, 19 Feb 2002).

One advantage to the TNA and PFNA technologies is that its computer analyzes the signals automatically and alerts operators if it detects the presence of drugs or explosives, removing the operator from the decision making process (Brown, 19 Feb 2002). The other advantage is that the detection determination does not rely on shape and is immune to diligent packaging. TNA and PFNA both provide a better alternative to low and high-energy technologies that require operator interpretation of what an image is representing (Gozani, 12 Mar 2002) (see Figures 4.35 and 4.36).

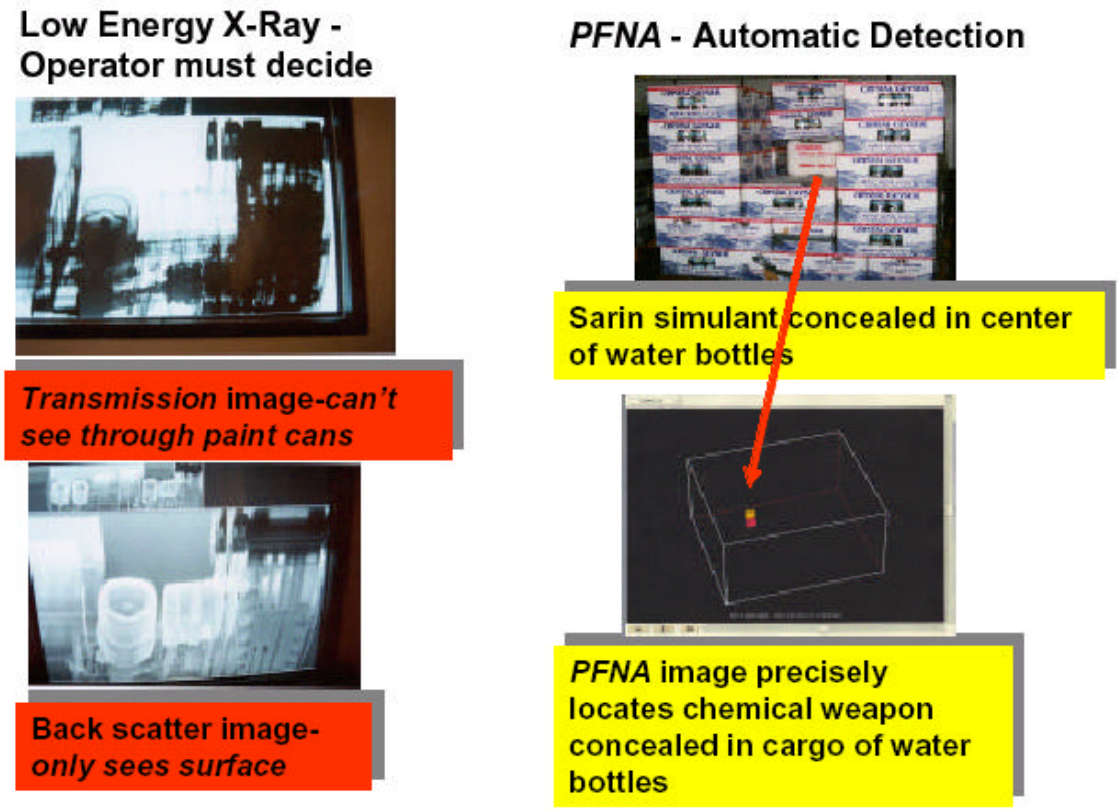


Figure 4.35. Comparison of Low Energy X-Ray and PFNA Technologies. (From: Gozani, 12 Mar 2002).

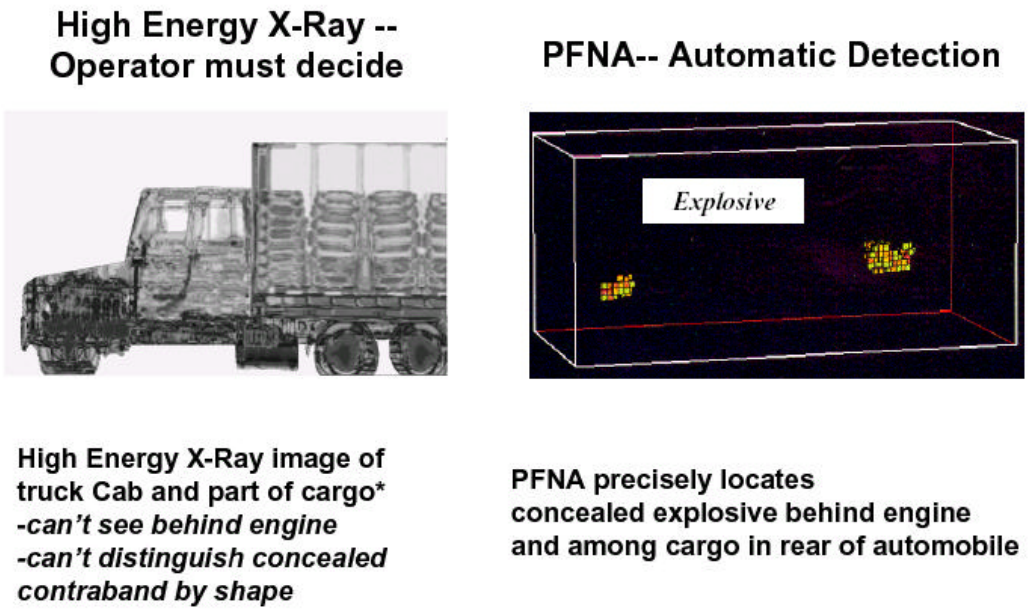


Figure 4.36. High Energy X-Ray and PFNA Technology Comparison. (From: Gozani, 12 March 2002).

Ancore has two PFNA products available that could be used as highly effective non-intrusive tools to detect explosives, narcotics, chemical weapons, environmentally hazardous materials, and specific dutiable goods. The Ancore Cargo Inspector (ACI) (see Figure 4.37) can be effectively used to inspect air cargo and passenger luggage, full-size marine cargo containers, loaded freight trucks, freight trains, and passenger cars.

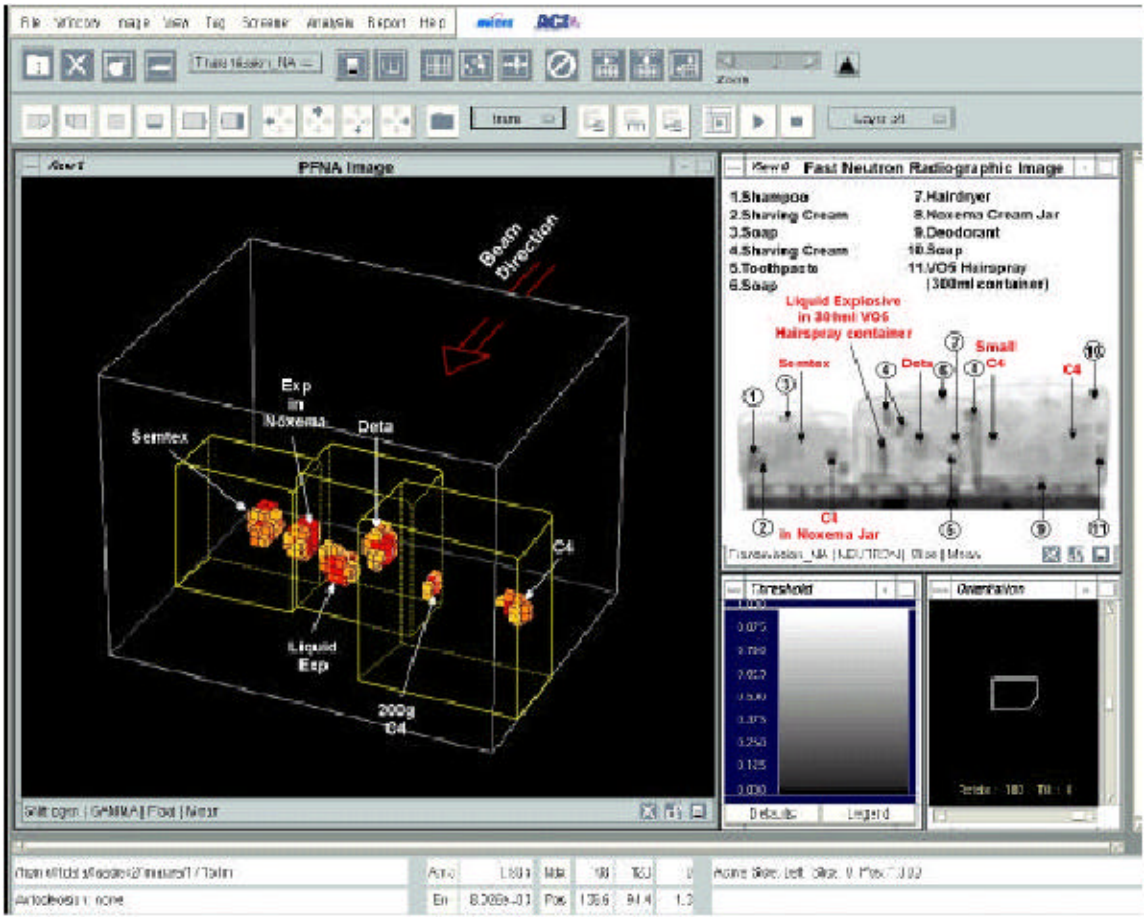


Figure 4.37. Ancore Cargo Inspector. (From: Gozani, 12 Mar 2002).

Ancore Corporation's Vehicular Explosive Detection System (V-EDS) (see Figurer 4.38) is a non-invasive tool, which can be used from a distance of several feet to detect explosives hidden in cars or trucks.

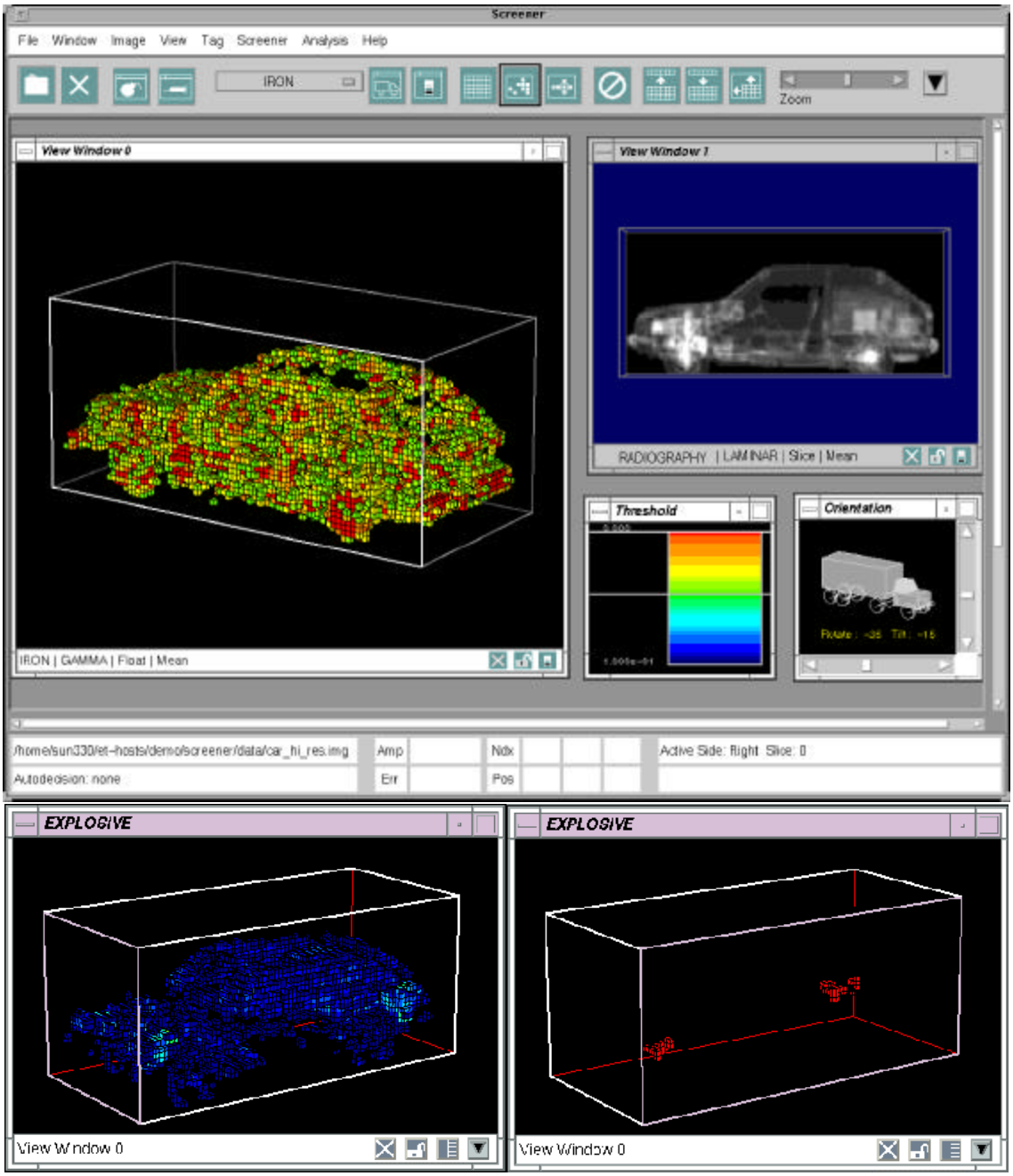


Figure 4.38. Vehicular Explosive Detection System (V-EDS). (From: Ancore.com, 2002).

2. Sniffers

a. Explosive Trace Detector (ETD)

Airport security personnel are using ETDs to detect minute particles of drugs or explosives that may be present in luggage. Security personnel wipe a swab or

pad over luggage and insert the sample into a machine that quickly checks for such particles (see Figure 4.39). ETDs are also are being used at embassies, police departments, prisons, nuclear power plants, and other high-security environments throughout the world (Orenstein, Nov 2001).

Figure 4.39. Explosive Trace Detector. (From: Barringer.com).

b. Personnel Sniffers

As part of a pilot program, the Federal Aviation Administration (FAA) installed EntryScan (built by Ion Track Instruments and Barringer Technologies) at McGee-Tyson Airport in Knoxville, Tennessee. Another device being tested by the TSA is a telephone booth-sized Barringer IonScan Sentinel II (see Figure 4.40) (Masterson, 3 Apr 2002). When travelers pass through the IonScan Sentinel II device shoots short burst of air to dislodge and disperse microscopic particles from the skin and clothing (Orenstein, Nov 2001). The microscopic particles are the vacuumed by the device. The Sentinel II then sniffs and analyzes the particles for traces of explosives, chemicals, or drugs. Ionscan type machines can be adjusted to test for 60 types of drug residues (Masterson, 3 Apr 2002).

Figure 4.40. Barringer's IONSCAN Sentinel II. (From: Barringer.com, 2002).

D. OTHER UBIQUITOUS SURVEILLANCE TECHNOLOGIES

Video surveillance tools, biometric technologies, scanners, and sniffers should not be the only "silver bullets" used in the battle to counter terrorism. Along with the technologies listed above, the following technologies are also being considered to make up a complete ubiquitous surveillance system.

1. Scoping Out Terrorists

- National/Travel/Visa/Passport Biometric ID Cards that use biometric technologies such as fingerprint, iris, and facial recognition—to reduce fraudulent identification, and automatically detect individuals who are suspected terrorist, criminals, or have expired visas.
- Unmanned armed CIA Predator aircraft—to fly over areas, gather intelligence, take reconnaissance photos, and take action as required.
- Reconnaissance and communications satellites—to monitor terrorist movements and communications.
- Electronic surveillance programs, such as ECHELON, and Carnivore (see Figure 4.41)—to ease-drop on terrorist communications.

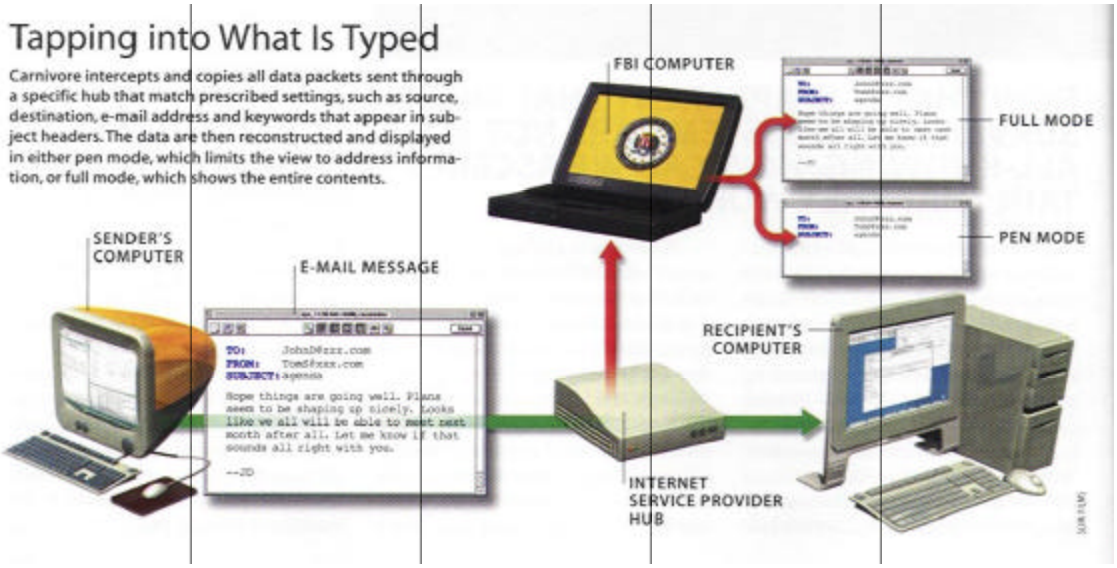


Figure 4.41. Carnivore. (From Hogan, Dec 2001).

- Enclosed Space Detection System (ESDS) —to detect the presence of persons hiding in enclosed spaces of vehicles or cargo containers (see Figure 4.42). The system operates by detecting the presence of the human ballistocardiogram, or small but measurable shock wave produced by the heart and propagated through the body and to surfaces the body is in contact with (DePersia, p. 140).

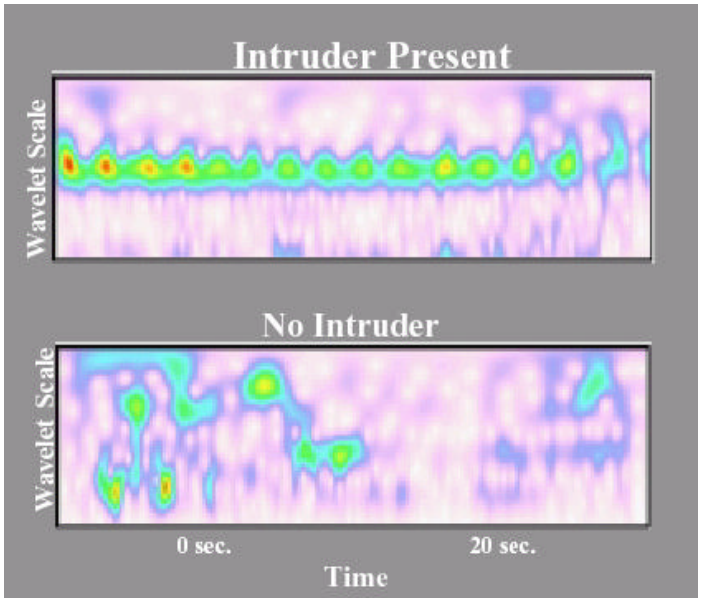


Figure 4.42. Enclosed Space Detection System. (From: ORNL.gov, 2002).

- Acoustic surveillance—to protect against "diving terrorists."
- Real time, peer-to-peer computing networks—to share information, obtain assessments, and coordinate actions.

2. Scoping Out Weapons

- Biological surveillance systems, such as dogs and sea mammals.
- Low Frequency Magnetic Imaging (LFMI) systems—to detect concealed weapons (De Persia, p. 108).
- In a project sponsored by the Department of Justice, Trex Enterprises is developing a passive millimeter wave camera (see Figure 4.43) to distinguish between body heat and heat given off by objects a person is carrying to detect hidden weapons (Tarquinio, p. 74).

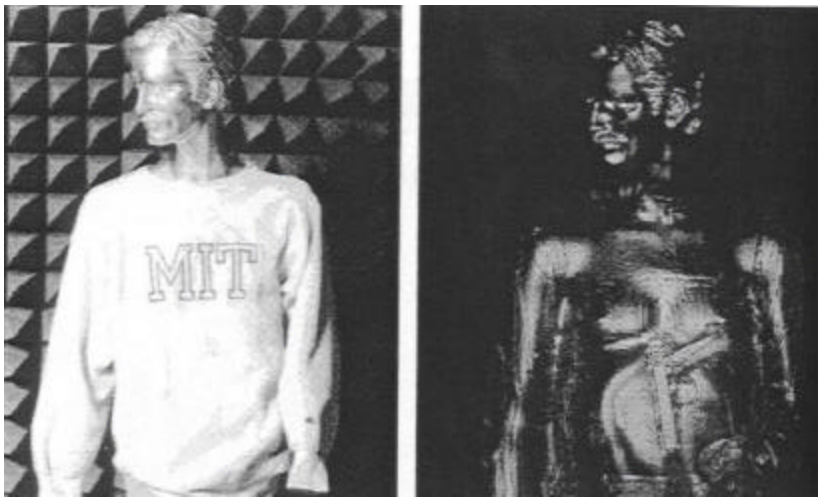


Figure 4.43. Millimeter Wave Camera Image. (From: DePersia, p. 123).

- Explosives and Nuclear Portals, being developed by the Department of Energy's Los Alamos and Sandia National Laboratories—these machines scan individual's who walk through them and are sensitive enough to detect the presence of both explosives, even small traces due to handling, and nuclear materials.
- Department of Energy's Idaho National Engineering and Environmental Laboratory is developing neutron source locating systems that can be used to collect real-time data to allow analysis of trends. Tests have already shown that putting just three sensors in motion could cover about 98% of a small city.
- Department of Energy's Idaho National Engineering and Environmental Laboratory is developing portable X-ray tomography systems. These

systems create three-dimensional images of contents and make dangerous items clearly identifiable (Tarquinio, Jun 2002).

- Acoustic surveillance sensors widely distributed over a community or threat area—used to triangulate gunfire or explosion location (see Figure 4.44) and prompt police and emergency response officials (DePersia, p. 130).

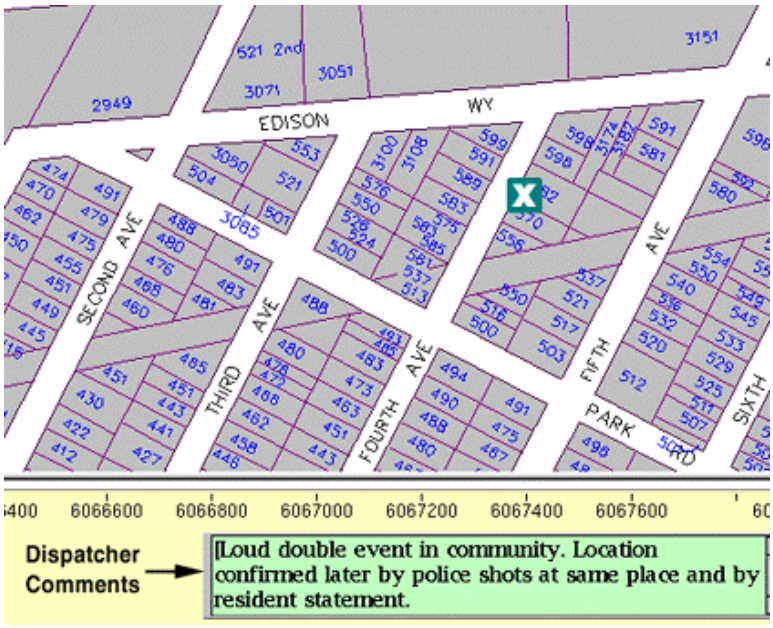


Figure 4.44. ShotSpotter. (From: ShotSpotter.com, 2002).

3. Safeguarding Cargo at Borders and Homeland

- Ship and Truck Transponders—to track location and routes taken.
- Accelerator Nuclear Materials Detector is being developed by the Department of Energy's Los Alamos and Idaho labs, in partnership with Aracor, to detect radioactive materials such as uranium or enriched plutonium (Tarquinio, p. 76).

4. Addressing the Biochemical Threat

- Rapid Syndrome Validation Project is being developed by the Department of Energy's Sandia Lab to allow doctors to enter symptoms into a computer network and immediately find out if similar cases are being detected by other doctors and what is know about those symptoms and its source. By monitoring such a network, epidemiologist at national, state, and local levels can detect problems and take action as appropriate (Tarquinio, p. 76).

- Health Alert Networks and a National Medical Intelligence Database are being developed to provide better data infrastructure to link emergency rooms, physicians and public health departments, and serve as an early warning system for public health crisis and bio-terrorism (Tarquinio, p. 77).
- National Institute of Health (NIH), John Hopkins University's Center for Civilian Biodefense Strategies, and other research institutions are developing DNA Chips to identify DNA structures of biochemical agents (Tarquinio, p. 77).
- Autonomous Pathogen Detection Systems are being developed by the Department of Energy's Lawrence Livermore National Laboratory to test air particles for signs of contaminants. These systems could be built directly into a building's ventilation system (Tarquinio, p. 76). A U.S. Department of Defense bio-agent to monitor and test the air for pathogens (see Figure 4.45) is also near deployment (Talbot, Dec 2001).

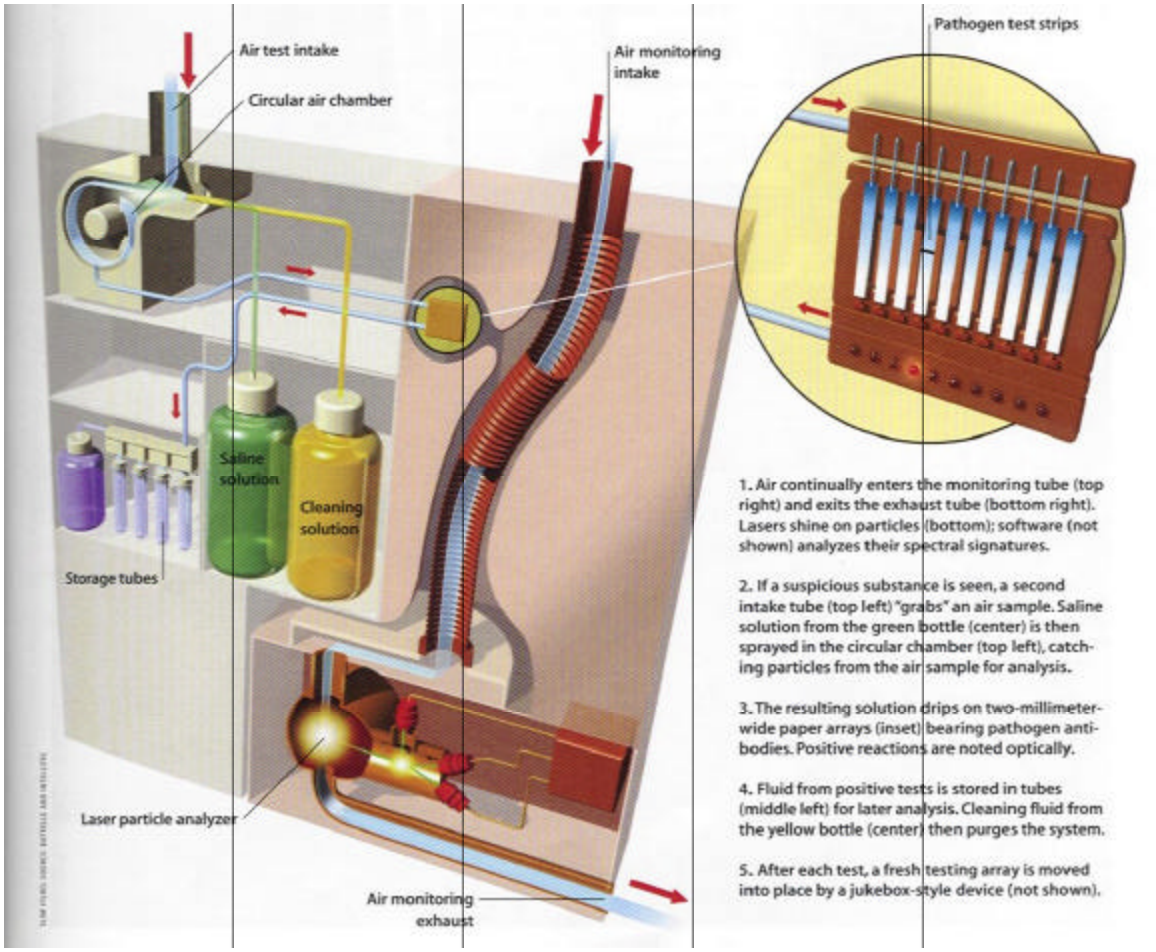


Figure 4.45. DOD's Bio-Agent Detector. (From: Talbot, Dec 2001).

- MIT's Lincoln Laboratory is developing Canary Chips to detect biological or chemical attacks (Tarquinio, p. 77).
- Department of Energy's Oak Ridge National Laboratory is developing Block II Chemical and Biological Mass Spectrometers to analyze both air and liquid to identify potential threats (Tarquinio, p. 76).
- Department of Energy's Sandia National Laboratories are developing soil and ground water chemical sensors to help detect deadly chemicals being dumped in small reservoirs. These sensors allow detection of chemical agents on-site and signal an alarm at a remote location (Tarquinio, Jun 2002).

Although there is no foolproof technical fix to counter terrorism, ubiquitous surveillance technologies and biometrics could significantly aid in the battle against terrorism (Woodward, Dec 2001). The challenge will be in determining the most effective ways to leverage these technologies to aid in prosecuting the war against terror.

THIS PAGE INTENTIONALLY LEFT BLANK

V. APPLICATION AREAS FOR SURVEILLANCE AND BIOMETRICS

The rise of networked, non-state terrorists requires the United States to change its national strategy. The U.S. government must understand that to beat a network one has to fight as a network. The strength of a network depends on how well it functions in the organizational, narrative, doctrinal, technological, and social levels (Arquilla, p. 324). New strategies must strengthen our ability to perform as a network at each of these levels. Strategies must also hinder on how well the adversary performs at each level. The rise of networked non-state actors requires the U.S. and its departments and agencies to evolve into hybrid all-channel networks (see Figure 5.1) in order to conduct "netwar" against this new type of adversary. All-channel networks allow improved collaboration and prevent stove piping of information.

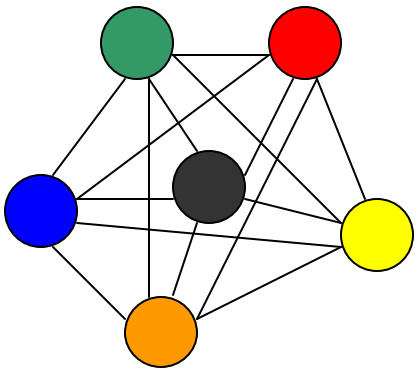


Figure 5.1. All-Channel Network. (From: Arquilla, p. 8).

Biometric and surveillance technologies provide both offensive and defensive tools that work in the technology-level of this war. They allow us to monitor changes in the adversaries use of information technology, target information flows, deer offensive operations by the networked actors by providing better security infrastructure, and allow the U.S. to work more efficiently as a network, thus beating non-state actors at their own game (Arquilla, pp. 52-54).

Changes in U.S. and international surveillance laws in the wake of the 9-11 attacks have allowed the U.S. and its allies to round up various al Qaeda terrorist cells

worldwide. Because of the success of the U.S. campaign against al Qaeda in Afghanistan, however, al Qaeda leadership has authorized its operative to ally themselves with helpful Islamic extremist groups (Priest, 30 Jun 2002). With al Qaeda reaching out to other terrorist groups, such as Hezbollah, to coordinate explosives and tactics training, money laundering, weapons smuggling, and the acquisition of forged documents (Priest, 30 Jun 2002), much still needs to be done to secure the homeland. As President George W. Bush has stated, this is a long war; and sleeper cells may already be in the United States waiting to strike. The following is an outline of various present and future applications of ubiquitous surveillance and biometric technologies, but they are only a small fraction of the actual deployments to date.

A. GOVERNMENT

Prior to 9-11, both surveillance and biometric technology were limited in use in the United States. Surveillance technologies saw limited use, because the threat against the homeland was not deemed significant. Therefore, their use was primarily limited to security applications in the private sector. Biometric technologies were slow to catch on because of the high cost and enormous computing power required to build accurate systems. The overall market for biometrics was approximately $325 million in 1999 (Evangelista, 21 Feb 2000). However, the combination of the growth in PC computing power, evolution of proprietary adaptive algorithms, lower-cost infrared optics, advances in digital imaging, and improved measurement methods enabled manufacturers to create biometric and surveillance devices for mainstream applications at a lower cost. Biometric and surveillance technologies emerged as a practical, effective solution for law enforcement, security, and fraud-free e-commerce. Biometric technologies aid in preventing identity theft and attendance fraud. According to industry analysts, the worldwide biometrics market will reach $10 billion by 2003 (I/O Software, Jun 2002).

Before 9-11, there were many initiatives to use biometric products by both the public and private sectors in various applications. The U.S. government had already invested heavily in biometrics technology research. A General Accounting Office (GAO) study ordered prior to July 31, 2001 to investigate the total Federal funds spent on researching biometric technologies revealed an expenditure of over $50 million, with $47

million being spent on facial recognition technologies (see Table 5.1) (Sullivan, 15 Apr 2002).

	U.S. Department				
Year	**State**	**Energy**	**Justice**	**Defense**	**Total**
Pre-1997	$0	$125,000	$3,668,000	$5,730,000	$9,523,000
1997	$0	$0	$4,843,000	$744,000	$5,587,000
1998	$0	$0	$5,500,000	$3,171,000	$8,671,000
1999	$12,000	$400,000	$787,000	$2,872,000	$4,071,000
2000	$450,000	$0	$784,000	$7,330,000	$8,564,000
2001	$100,000	$0	$5,709,000	$4,843,000	$10,652,000
Total	$562,000	$525,000	$21,291,000	$24,690,000	$47,068,000

Table 5.1. Facial Recognition Spending by Departments Prior to July 31, 2001. (From: Sullivan, 15 Apr 2002).

Although twelve different government agencies had funded or conducted research on biometric technologies, the study revealed that only one agency reported it had actually deployed the technology. The resistance to deploy biometric and surveillance technologies was greatly due to pressures felt from privacy groups.

Although biometric technology is a popular choice among agencies since the 9-11 terrorist attacks, some biometric technologies require further testing to ensure that they are appropriate and effective for the given application. Both privacy and technical issues have caused the GAO to caution agencies that are considering biometric applications that the new Patriot Act does not give them authority to start applying these technologies. The GAO is suggesting that agencies conduct more research on each technology to figure out which technologies are best and where they would be best applied. The GAO is also encouraging agencies to think about how these systems might be evaded and develop methods to guard against such evasion. Agencies also need to consider layering technologies. By mixing the use of biometric technologies with tokens, smart cards, PINs, passwords, and multimodal biometric systems, authentication processes can be strengthened. The objective in using biometric technology is not to replace security personnel but to aid agencies in identification and authentication during a time when identifying identity theft and terrorism is growing (Bhanbhani, 3 Jun 2002).

New bills signed to promote homeland security have brought about many new deployments of surveillance and biometric technologies. Biometric and surveillance technologies are now being tested for an increasing number of applications under the most challenging and demanding conditions at the Defense Department's Biometrics Fusion Center. The center is reporting each device's strengths, weaknesses, and suggested uses to the Biometrics Management Office at the Pentagon (Bhambhani, 15 Jul 2002). The center is currently conducting field tests of nine fingerprint products, two iris scanners, and one hand geometry reader (Jackson, 22 Jul 2002).

Biometric devices are now being deployed to protect facilities that are vital to national security, prevent unauthorized people from crossing borders, and preserve the integrity of our critical infrastructure: financial systems, power grids, air control, and data networks. Real-world applications of biometric technologies have shown that its products are robust, easy-to-use, and cost-effective. As new needs continue to be identified, the practical applications of biometric and surveillance technologies will expand. In this war against terror, the application areas are primarily in law enforcement, security, physical access control, and network access control. The biggest challenge remains settling on a specific identifier for each application.

1. National ID Card and Driver's Licenses

Immediately after the 9-11 attacks, Oracle Corp. chairman Larry Ellison offered to provide the software for a national ID system free of charge (Scheeres, 25 Sep 2001). Ellison has since said he favored a national standard for current ID data. Though no single member of Congress has spoken out in favor of a universal ID card, tech company representatives have shown their products to various government subcommittees. The U.S. is not the only country debating the use of a national ID card. The Dutch government is also studying the integration of their national identification card with biometrics (I/O Software, Jun 2002). Some members of the UK government are pushing for a national ID card after launching early in 2002 a chip-based biometric ID cards to document the tens of thousands of asylum seekers that come into their country every year (CardTechnology.com, 8 Jul 2002). Iris and fingerprint biometric technologies show the

best promise for application with a driver's license, national ID, visa, passport, or frequent traveler ID card.

Another key hurdle in information strategies and prevention is the driver's license, which is issued by states and generally accepted in other states as valid identification. Rules for issuance vary greatly from state to state. Although none lived in Virginia, seven of the 9-11 hijackers had Virginia driver's licenses and used them to board airplanes, use credit cards, and open bank accounts. Both falsified and legally obtained driver's licenses can be used as a gateway to criminal activity. The U.S. government should discuss with states the need to develop standardized rules for issuing licenses and require biometric templates and digital pictures on all licenses (O'Hanlon, Summer 2002). Biometrics can turn a questionable driver's license into a secure identification card that can be relied upon to identify a licensed individual. Biometric technologies can also be used to conduct background checks on, and create secure identification cards for, workers who have access to cargo, hazardous materials, and shipping goods. Initiatives are underway among some states and national governments to use biometric technologies to aid in detecting and eliminating duplicate driver's licenses and verify the identity of license holders.

2. Government Facilities

Government facilities contain sensitive materials, critical data, high-ranking officials, and sensitive information. For this reason, positive identification of all personnel is required.

a. Common Access Card

Biometric technologies are part of a redesigning of the Department of Defense (DOD) Common Access Card (CAC). DOD is issuing the Common Access Card (CAC) to 4.3 million active duty U.S. military personnel and eligible contractors (Bhambhani, 6 May 2002). Figure 5.2 shows the DOD's timeline for the biometric cards. DOD's biometrics program is now a line item in the DOD budget proposals for fiscal 2004 through 2009 (Jackson, 22 Jul 2002). The Biometrics Fusion Center is currently evaluating 56 biometric products—25 fingerprint devices, eight facial recognition systems, two iris scanners, two hand geometry scanners, two speaker recognition

systems, one signature recognition system, one iris scanner, 14 middleware products, and a Web portal (Jackson, 22 Jul 2002).

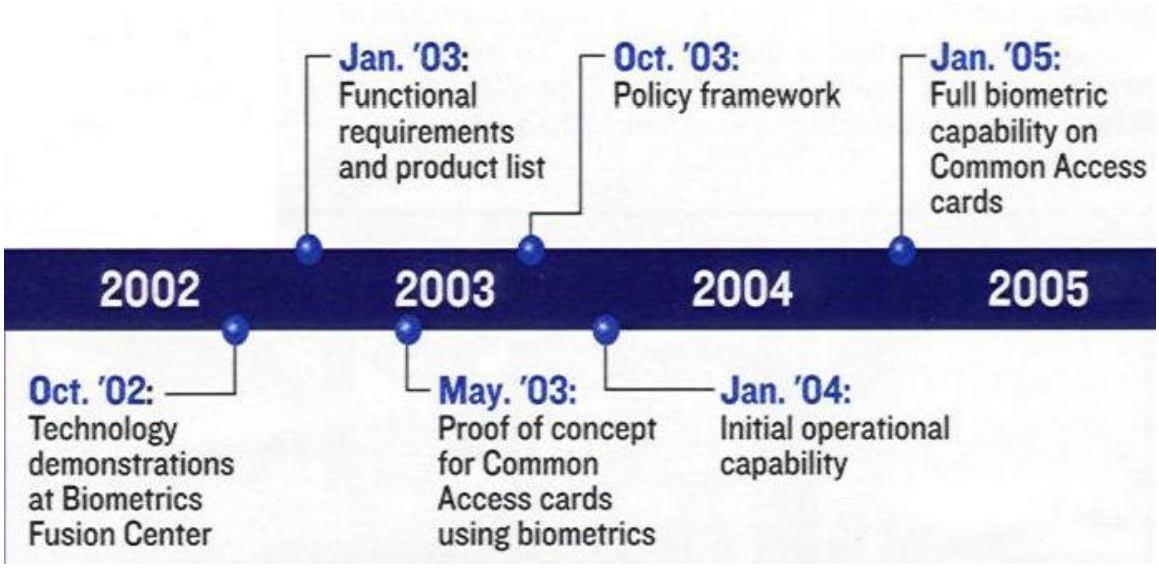


Figure 5.2. DOD's Timeline for the Secure Installation Access Control System. (From: Jackson, 22 Jul 2002).

b. CCTV and Facial Surveillance

Washington D.C. Mayor Anthony A. Williams has said increased government surveillance is a reality of post-September 11 world and thinks Washington D.C. needs to follow the lead of cities such as London, England and Sydney, Australia and expand its camera system (ObservingSurveillance.org, Jun 2002). Figure 5.3 shows how the National Park Service has deployed around-the-clock video surveillance at all major monuments on the Mall and throughout buildings of interest throughout Washington, D.C. (Hsu, 22 Mar 2002).

Figure 5.3. Surveillance Camera Infrastructure in Washington D.C. (From: ObservingSurveillance.org, Jun 2002).

Abu Zubaida's interrogations led to increased surveillance at some of New York City landmarks. Since in the course of his marathon debriefings he stated that al Qaeda cells had discussed attacking "the statue in the water," a facial-recognition surveillance system was deployed to take pictures of visitors to the Statue of Liberty and Ellis Island as they board ferries. It is comparing the images with those in a database of suspected terrorists provided by the FBI (Kugler, 27 May 2002).

3. Military

a. Aerial Surveillance

The use of various military and government surveillance platforms have made great contributions in the war against terror. The CIA has used its RQ-1 Predator UAV (see Figure 5.4) extensively in operations in Afghanistan. The Michigan National Guard wants $4 million in funds to acquire a Predator spy plane to monitor infiltrations

from Canada (Newman, 31 Mar 2002). What makes the RQ-1 Predator an invaluable tool for surveillance and reconnaissance is its long endurance, over 40 hours, and its surveillance imagery capability: synthetic aperture radar, video cameras, and a forward-looking infra-red (FLIR). Surveillance images can be distributed in real time via satellite communication links to the front line soldier, the operational commander, or worldwide. (Army-Technology.com, 2002) RQ-1 Predator is also evolving into a strike platform.

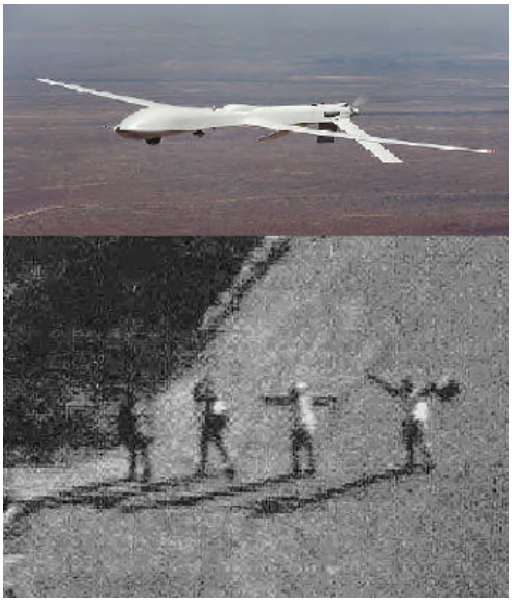


Figure 5.4. RQ-1 Predator UAV with a Product. (From: FAS.org, 22 Jun 1996).

Aerial surveillance platforms patrolling the northern Arabian Sea, such as P-3C Orion aircraft, are being used as part of the massive dragnet, Leadership Interdiction Operation (LIO), aimed at hunting down al Qaeda members who may be trying to flee Pakistan by ship. Orions have special infrared cameras that can spot human targets moving on the ground as well as vessels trying to maneuver in the dark without their running lights. The cameras are sensitive enough to detect the ship's wake.

U.S. aerial surveillance has also aided the Philippine government in its war against Abu Sayyaf, who has ties with al Qaeda. Abu Sayyaf extremist guerillas were tracked by U.S. surveillance planes on the southern island of Jolo in the Sulu province (MSNBC, 28 Jun 2002). Abu Sayyaf camps were also detected in Patikul town

and were raided by U.S. trained Philippine troops. The U.S. is also supplying the Pakistani government with five U.S. helicopters fitted with sophisticated communications and surveillance technologies and three surveillance planes to aid in monitoring its tribal regions for al Qaeda and Taliban operatives (Associated Press, 5 Jul 2002). Other aerial surveillance technologies undergoing testing include:

- *Global Hawk* (see Figure 5.5) – High-altitude, long-range UAV with cameras, infrared sensors, radar, jamming equipment and with 42-hour endurance.

Figure 5.5. Global Hawk. (From: Associated Press, 12 Jul 2002).

- *CamChopper* (see Figure 5.6) – Small-scale helicopter with video camera, infrared imager, small payloads, 6-hour endurance, and controlled via laptop-style ground station (Associate Press, 12 Jul 2002).

Figure 5.6. CamChopper. (From: Associated Press, 12 Jul 2002).

- *Micro Air Vehicles (MAV)* - DARPA is funding development of small flying machines for military intelligence, such as the Black Widow (see Figure 5.7). Endurance for MAVs is typically 30 minutes (Associate Press, 12 Jul 2002). MAVs provide unique surveillance capabilities in both the urban areas and the battlespace (see Figures 5.8 and 5.9). MAVs could aid in preventing civilian casualties by allowing identification of

friend or foe. MAVs could also be used to detect the makeup and direction of chemical clouds.

Figure 5.7. Black Widow MAV. (From: Associate Press, 12 Jul 2002).

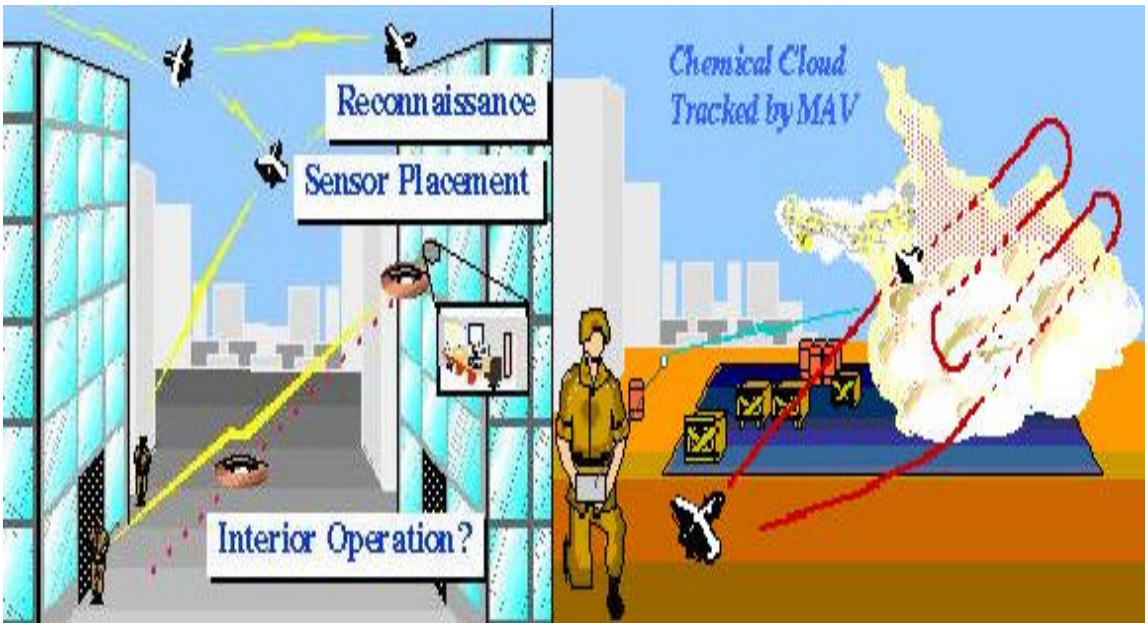


Figure 5.8. Micro Air Vehicle Surveillance Applications in Urban Areas. (From: McMichael, 7 Aug 1997).

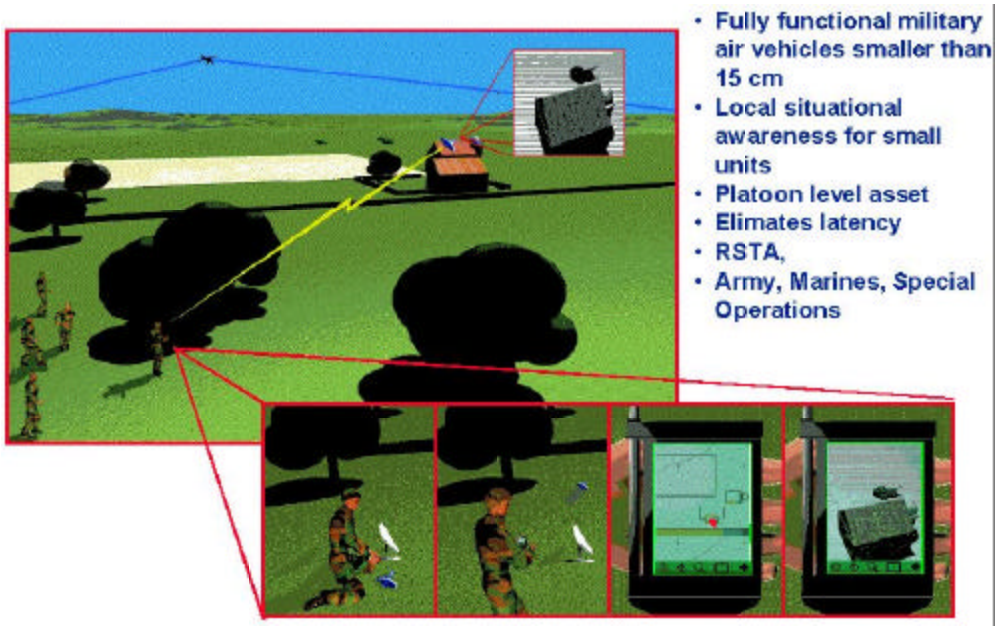


Figure 5.9. MAV Surveillance Applications in the Battlespace. (From: Wilson, 30 Jun 1998).

- *Micromechanical Flying Insect* (see Figure 5.10) – biologists and technologists at the University of California, Berkeley are trying to develop a tiny robot that will flutter like a fly. DARPA is funding much of the work because of its potential application in both reconnaissance and surveillance (CNN.com, 28 Jul 2002).

Figure 5.10. Micromechanical Flying Insect. (From: Associate Press, 12 Jul 2002).

b. Pier Access Control

The U.S. Navy is integrating Viisage's FacePASS system into a mantrap environment to limit access to one person at a time to the Submarine Base Point Loma pier. This is being done to investigate whether or not a move from a manned facility to

an unmanned facility during off hours. Cindy Milholland, a project engineer at Point Loma, stated, "Our initial findings have been promising. In the present environment, the system is performing the job of access control very well." (BiometriTech.com, 8 Jul 2002).

c. Communication Surveillance

U.S. Navy submarines are playing a critical role in gathering intelligence about the al Qaeda terrorist network by intercepting telephone conversations and by other means. Their capabilities are in high demand by both the Pentagon and CIA, and their missions have risen 30% since 9-11. They provide one of the best tools for gathering intelligence information because they are stealthier than unmanned aerial vehicles and cannot be tracked the way surveillance and communication satellites can. The rise in missions, however, has reduced the projected service life of the submarines' nuclear cores (Jaffe, 26 Jun 2002).

4. Immigration and Border Control

Immigration, travel, and border control are some of the key areas in which biometrics and surveillance technologies are gaining acceptance and are being applied to fight this new war on terror at home. Prior to 9-11, little was being done to administer a strong program to secure the gateways to the country. The legacy of an open society and the naïve assumptions that the U.S. homeland was immune to terrorist attacks allowed the toleration of large porous borders and the use of fragmented administration systems. In just the year 2000, 489 million people, 127 million vehicles, 11.6 million maritime containers, 11.5 million trucks, 2.2 million railroad cars, 829,000 planes, and 211,000 vessels passed through U.S. border inspection systems. In addition, 100,000 temporary work visas and 280,000 student visas were issued by the State Department. About half of the 7 to 8 million illegal immigrants in the United States have overstayed their student or tourist visas (Lodal, 1 Apr 2002).

The U.S. Enhanced Border Security and Visa Entry Reform Act of 2002, signed by the President on 14 May 2002, seeks to eliminate the vulnerabilities of the U.S. immigration system and border security. Some highlights of this new law include:

- INS shall install biometric readers to scan biometric documents at all ports of entry to the U.S. by 26 Oct 2003.

- State Department shall issue visas and travel documents to international visitors that are tamper-resistant and machine-readable using biometrics by 26 Oct 2003.
- All planes and ships arriving from abroad must submit in advance passenger and crew list or manifests.
- All countries that want to continue to take part in the U.S. Visa Waiver program are required to issue biometric embedded passports to its nationals.

a. Passport and Visa Issuance

Processing an increasing number of legitimate travelers and visa applicants while at the same time identifying lawbreakers, has put a major a strain on immigration authorities and transportation security screeners around the world. To allow these authorities to quickly and automatically process law-abiding travelers and identify illegal immigrants, terrorist, drug-runners, and people involved in identity theft, new systems are being deployed throughout the U.S. and internationally. The INS has stipulated that it could each day detect and deter about 3,000 illegal immigrants crossing the Mexican border without delaying the legitimate people entering the United States if it had a quick way of establishing positive personal identification. (I/O Software, Jun 2002)

The Immigration and Naturalization Service (INS) and the Justice Department are now becoming major users and evaluators of biometric technologies. The objective of using biometric technologies is to deter and prevent illegal aliens holding false visas, forged passports, stolen papers, or copied documents from entering the country (Polemi, p. 32). Another objective is to identify individuals who have overstayed their student or tourist visas. Biometrics technologies and other technologies are being employed in a number of diverse applications and include:

- The U.S. Immigration and Naturalization Service Passenger Accelerated Service System (INPASS), in place since 1993, is an automatic passport control system that is being used to verify passengers at transportation hubs (Polemi, p. 32). It allows frequent international travelers to bypass waiting lines in the airport. Approximately only 0.64 percent of the total international travelers were enrolled in 1999. It uses Recognition Systems' hand-scan technology. There are approximately 50,000 active users of the kiosk-based hand-scanners. The system is in operation in New York, Newark, Washington-Dulles, Miami, Los Angeles, San

Francisco, and U.S. pre-clearance hubs in Vancouver and Toronto (Nanavati, p. 102).

- The U.S. Customs Service's (USCS) legacy Automated Customs System (ACS) is being replaced with the Automated Customs Environment (ACE) (5 years, $1.3 billion). ACE is operational in three border stations, right now, and should be fully deployed by 2004. ACE was designed only to reduce the paperwork associated with border crossings and does not interface with the FBI's National Crime Information System (NCIS). The USCS is spending over $1 billion to keep ACS running while ACE is being developed (Lodal, 1 Apr 2002).
- The Justice Department is developing a program that will fingerprint and photograph aliens of national security concern, who meet as-yet-unidentified criteria (but may include country of origin). Foreign individuals holding visas in good standing would also be asked to come in for fingerprinting and photographs. INS's Computerized Applicant Information Management System already holds photographs of aliens and has been modified to hold fingerprints. However, INS lacks the staff and resources to operate the system at all 300 ports of entry (Dizard, p. 15).
- The U.S. State Department is planning to develop a visa tracking system, which would create alerts on visas that had expired to keep track, which visa holders are overstaying on the visas. It should eliminate passport and visa fraud and digitize existing photographs (Bhanbhani, 3 Jun 2002).
- As the first step in the government's plan to track temporary student visas, the INS has launched a Web site system called SEVIS to register foreign students. The system will become mandatory at campuses nationwide on 30 Jan 2003. The system is being implemented to close many loop holes that have led to the government's losing track of foreign visitors with student visas by ensure that they actually are attending school and not heading off to places unknown. Using the Web site, campuses would report when the student arrived, course of study, and any changes in the field of study. If the student never shows up or disappears, the INS would then try to track down the foreign student with law enforcement agents (Associated Press, 2 Jul 2002).
- A pilot program called CANPASS was deployed to ease and secure the passage of goods and services across the U.S. and Canada northern border. Only low-risk U.S. and Canadian citizens can register for CANPASS. CANPASS uses fingerprint technology (Nanavati, p. 102). The European Union (EU) is considering a similar program (Polemi, p. 32).
- The INS has recently been developing several new projects:
  - To comply with the INS Data Management Improvement Act, INS has requested $362 million for fiscal year 2003 to develop its Entry-Exit Visa System. The new system will integrate databases

used by the Customs Service, INS, State Department, and other agencies to track individuals entering and leaving the country (GCN, 24 Jun 2002).

- Working with the Transportation Department, INS is developing a Dedicated Commuter Lane System that will allow pre-approved frequent border crossers to enter the country without a border stop. The system will scan vehicles' unique identifiers or driver and passengers' biometric identifiers (GCN, 24 Jun 2002).

Biometric technologies are gaining widespread acceptance in Australia, Bermuda, Germany, Malaysia, Saudi Arabia, and Taiwan. King Fahd University of Petroleum and Minerals, in Saudi Arabia, plans to control access to its 900-acre campus with biometric technologies (CardTechnology.com, 9 Jul 2002).

b. Immigrant ID Verification

The INS is employing biometric technologies to aid in ensuring that immigrant documents are not tampered with. Facial and finger biometrics are being employed to verify that the name and photo on the document does belong to the same person and that the identity of the person holding the document matches the identity of the person who was issued the document. The INS has recently been developing several new projects to aid in keeping track of immigrant status (GCN, 24 Jun 2002):

- INS's Systematic Alien Verification for Entitlements verifies immigration and employment status for more than 50,000 users nationwide.
- INS's Verification Information System verifies and manages reporting of immigrant-status data to INS-approved users.
- The State Department has a biometric identification card system, which works under a special agreement with Mexico and gives about 6 million Mexican nationals legal access to the United States (Dizard, p. 15).

Although the new systems and upgrades provide advancements in the right direction, some major problems still exist. New INS systems currently only interface with the FBI's NCIS at two locations and do not interface with the INS border patrol system that uses biometrics to track illegal immigrants or the program that issues digital biometric green cards to resident aliens (Lodal, 1 Apr 2002). Fingerprint verification is the most popular biometric used in this application (Polemi, p. 32).

c. Mobile Identification

Verification of a person's identity should does not have to be done at a particular location, situation, or environment. At airports, borders, seaports, and other locations where security takes precedent, handheld wireless identification devices are available to perform this task (see Figure 5.11). They allow security personnel to conduct on-the-spot immediate identity verification checks.

Figure 5.11. IBIS Remote Data Terminal. (From: Identix.com, 2002).

d. Surveillance at Borders and Ports

The Coast Guard and the Customs Service are the agency elements that make up the nation's counterterrorism effort against illicit cargo hidden within containers at our borders, seas, and ports. Both are vital agencies in detecting and stopping explosives or WMD headed for the U.S. homeland on a cargo ship. Over 1,000 foreign-flag ships reach U.S. shores each week and present the Coast Guard with a huge challenge. The Coast Guard has been patrolling at over 100 security zones around major naval bases, key landmarks, oil refineries, prominent ports, and nuclear power plants along navigable waterways. To improve the security of vessels ashore, the Coast Guard is updating the National Distress and Response System (maritime 911 system), which monitors distress calls from vessels. Other new proposals being discussed, involving cargo container security, include databases that provide real-time tracking of containers headed to the U.S. that include certification of inspections by the companies shipping them, attached security devices that detect breaches in containers, and ship transducers to track ports of call before reaching U.S. shores or land borders (O'Hanlon, Summer 2002).

The U.S. Customs Service inspectors are using Radiation Detection Pagers (see Figure 5.12) to be alert when they are radioactive materials in their vicinity. These sensitive devices have a range of several hundred feet and classify radiation levels into a 1 to 10 scale. A detected strength level of 8 requires the inspectors to evacuate people from the area and to call hazardous material specialists. The Customs Service is also setting up isotope identifiers to distinguish the kinds of radiation being emitted—commercial, medical, or other radioactive materials (Gilot, 27 Jul 2002).

Figure 5.12. Radiation Detection Pager. (From: Gilot, 27 Jul 2002).

Some of the most promising products available to protect our borders with minimal effects on commerce and global trade include Ancore's ACI and V-EDS systems (see Chapter IV). Ancore's non-intrusive inspection systems can automatically detect explosives, chemical weapons, illegal drugs, and nuclear devices. Ancore has adapted its PFNA and TNA technologies for use at airports, seaports, and border crossings to inspect a range of objects, from shipping containers to cellular phones (Gozani, 12 Mar 2002). Drs. Douglas R. Brown and Tsahi Gozani of Ancore Corporation outlined conceptual ideas on how Ancore's PFNA and TNA technologies could best be used for air cargo, border, and seaport security (Brown, 19 Feb 2002 and Gozani, 12 Mar 2002). Ancore's V-EDS products (see Figures 5.13 and 5.14) could best be utilized at border crossings and weigh stations. Ancore's ACI could be used to develop a movable cargo inspection facility (see Figure 5.15) to be employed in ports (Gozani, 12 Mar 2002). A similar fixed scanning facility could also be developed for both border and port application (see Figure 5.16). American Science and Engineering Inc. has also developed specially equipped trucks that can scan unopened shipping for radiation emissions. It is currently courting

the U.S. Customs Service with their technology, but it is a hard sell at $2 million per unit (Gilot, 27 Jul 2002).

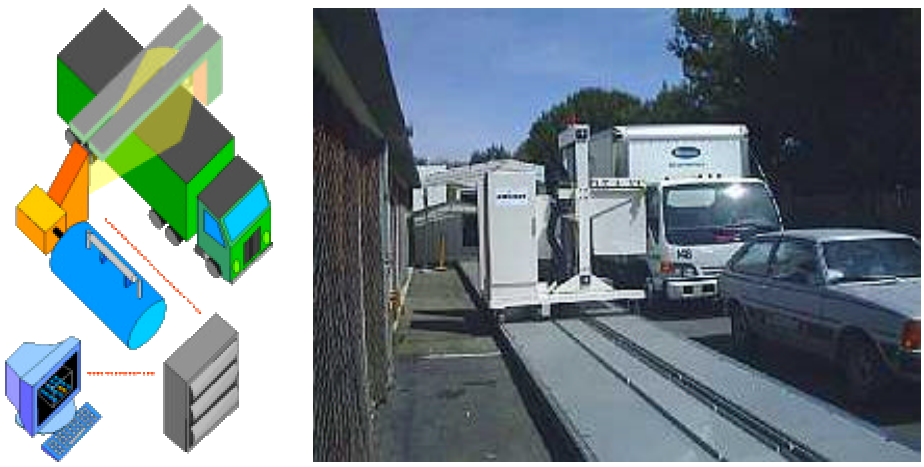


Figure 5.13. Ancore's Rail-Mounted V-EDS. (From: Ancore.com, 2002).

Figure 5.14. Ancore's Truck-Mounted V-EDS. (From: Wilson, p. 52).

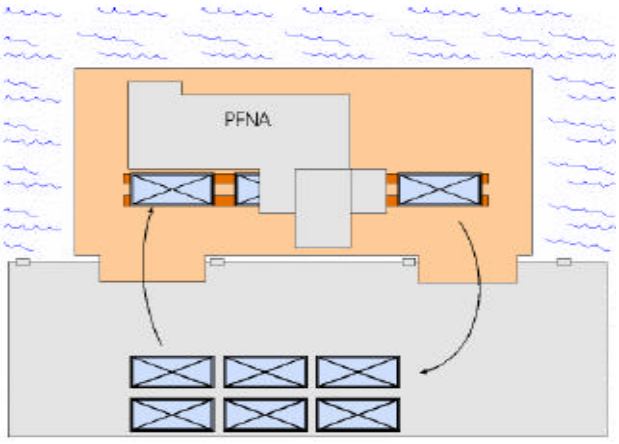


Figure 5.15. Mobile Cargo Inspection Facility for Ports. (From: Gozani, 12 Mar 2002).

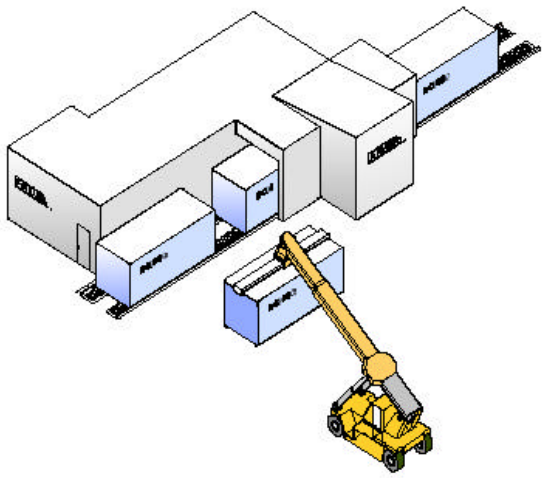


Figure 5.16. Fixed PFNA Land/Sea Cargo Scanning Facility. (From: Brown, 19 Feb 2002).

B. AVIATION

The challenge facing TSA is analyzing the security threats faced by airports and leveraging existing technologies to counter these threats. The TSA is also trying to develop effective surveillance and screening procedures that both provide security and reduce customer's waiting time. An airport is not only a transportation hub; it is also part industrial complex and shopping mall. With millions of law-abiding people flying on planes, there is always the possibility that a terrorist or criminal will try to hide among the masses with the intent to do harm. Threats to airport occupants could come from passengers, visitors, employees, cargo, and mail.

The TSA has addressed the various weak points at airports (see Figure 5.17) by applying increased biometric technologies, human surveillance, animal surveillance, scanners, and sniffers. The TSA is also examining lessons learned from applications abroad (Masterson 3 Apr 2002):

Figure 5.17. Applications at Airports. (From: Masterson 3 Apr 2002).

1. Vehicles

Currently, there is no reliable system in place to prevent someone from driving a bomb-laden car up the front drive and setting it off, but vehicles outside airports are being closely monitored. Packed, unattended vehicles are towed. Lessons from abroad include:

- Unattended or illegally parked vehicles are also towed in Europe and Asia.
- Vehicle monitoring extends to entry roads at several foreign airports.
- Tel Aviv's Ben Gurion International Airport uses checkpoints with armed guards and inspectors. They inspect documents for every car.
- At Narita International Airport in Tokyo, police and security personnel routinely inspect the underside of trucks and cars that arrive.

2. Outside of Airport

Currently, there are no security checks outside of most U.S. airports. Curbside and off-site baggage check-in are again becoming available in several cities, after being prohibited by the FAA in the aftermath of the 9-11 attacks. Lessons from abroad include (Masterson 3 Apr 2002):

- Curbside check-in is not allowed at most foreign airports.
- Armed undercover security officers patrol the area outside Ben Gurion International Airport in Tel Aviv. They stop and question passengers, then alert their colleagues inside the airport to any suspicious individuals.
- At Tokyo's Narita International Airport, police check the identification of every person entering the airport.

3. Ticket Counter

Due to the shootings at Los Angeles International Airport on 4 Jul 2002, the TSA is planning on placing armed uniformed and plainclothes officers at ticket counters and other areas of the airport as the first line of defense against a threat (Associated Press, 6 Jul 2002). One of the first lines of defense at airports is confirming a person's identity. This is currently being done with the use of a photo ID, such as a passport, military ID, or a driver's license.

One of the lessons learned from Italian investigations of convicted Egyptian terrorist, Abdelkader Mahmoud Es Sayed, also known as Abu Saleh, who headed al Qaeda's document committee based in Milan, was that al Qaeda has been successful in conducting clandestine movement of their terrorist cells by supplying them with a variety of false travel documents (Crewdson, 30 Jun 2002). To counter this, studies are being conducted to improve the verification of a person's identity by using biometric smart cards. Biometric Passport/Visa/Travel/ National ID card are being studied. Already, local and federal agencies use ID cards and databases in issuing Social Security cards, driver's licenses, passports and other identifications. A consolidation of at least some of those various IDs into one national card could make it harder for terrorists and criminals to pass through travel and immigration gateways. Proponents of National ID cards in the U.S. and UK have called for embedding biometric templates, such as finger and facial scans, into smart cards as part of a system (see Figure 5.18) that could be used at transportation centers (Scheeres, 25 Sep 2001). Using facial recognition technology in conjunction with installed CCTV cameras at airports, individuals can be checked against terrorist or criminal watch lists and manifests lists as they check in at a ticket counter, or disembark planes and approach customs or passport control areas.

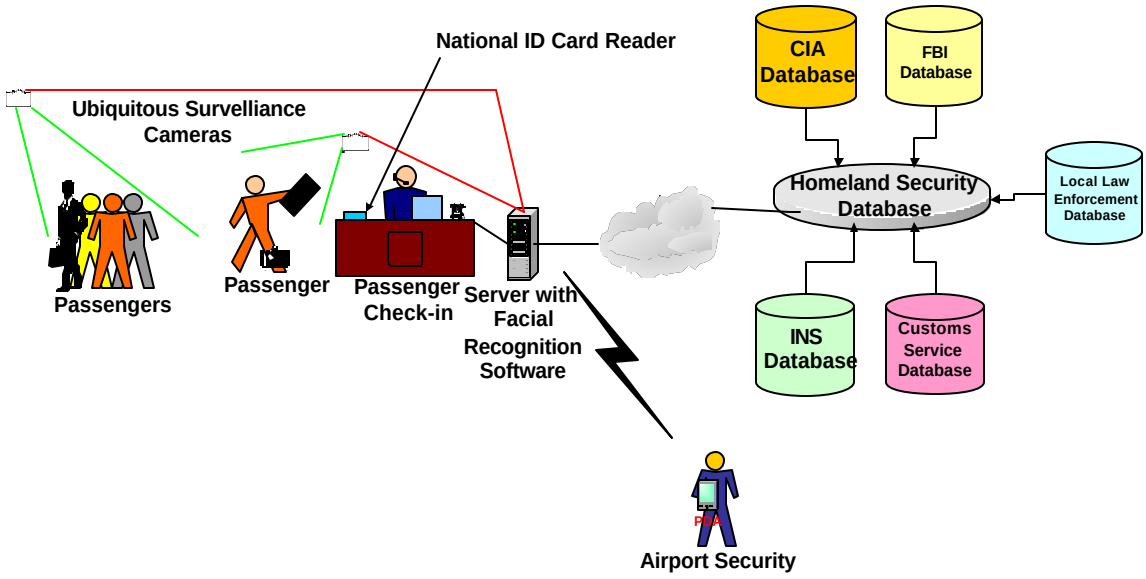


Figure 5.18. Ubiquitous Surveillance System at a Transportation Center.

Since testing and deployment of biometric technologies such as face recognition are supported in new airport-security bills, facial recognition systems are now being deployed to scan airport terminals for suspected terrorists. A government committee, appointed by Transportation Secretary Norman Mineta to improve airport security, received briefings from the leading facial recognition vendors: Visionics and Viisage. By installing hundreds of cameras at airports and connecting them via the Internet to servers running programs similar to Visionics' FaceIt program, airport security and other law enforcement agencies will try to identify terrorists and other criminals (see Figure 5.19). Safe-Travel is ready to launch its patented Secure Perimeter Identification System (SPIdS). The system defines the process of embedding real-time biometrics on airline boarding passes. The system is using fingerprint and facial-recognition systems from Imagis Technologies, Identix, Inc., and Digital Persona (BiometriTech.com, 5 Aug 2002).

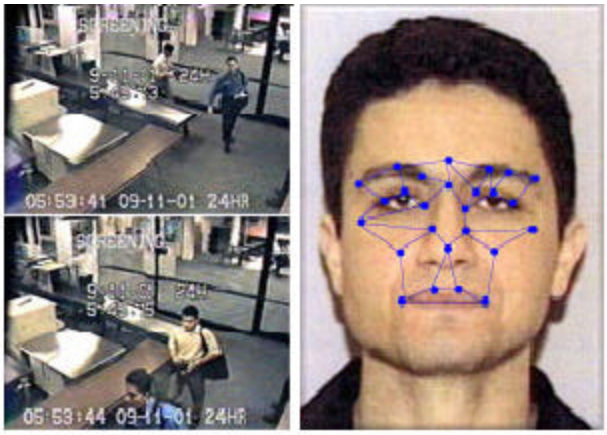


Figure 5.19. Video Surveillance with Facial Recognition. (From: Stikeman, Dec 2001).

Facial recognition systems by both of the companies listed above were tested at various airports with mixed results. Systems by both companies installed at Boston's Logan Airport, where two of the 9-11 hijacked flights originated, worked more than 90 percent of the time. These positive results contrast with a report on a similar test conducted at Florida's Palm Beach International Airport, which showed that a Visionics' system failed to work 52.5 percent of the time. Other tests conducted on a Visionics' system at Texas' Dallas/Fort Worth International Airport had a success rate of between 85 to 93 percent (Reuters, 16 May 2002).

The Aviation and Transportation Security Act requires that EDS screenings (see Figure 5.20) be in place for all checked baggage by Jan. 18. A total of between 2,000 to 3,000 detection systems need to be deployed to cover the 429 commercial airports across the country. The only two companies (Invision Technologies, Inc. of Newark, California, and L-3 Communications Corp. of New York) that are certified by the Federal Aviation Administration (FAA) to make the systems, do not have the production capacity to produce enough machines by the government deadline. Therefore, most experts believe that airlines and airports likely will miss the government's deadline. Many airports want to match bags with passengers in lieu of screening bags for explosives, but ensuring that checked luggage is cross-referenced against passenger manifests does not deter suicide bombers. Therefore, by 2003, passenger matching will no longer be allowed as an option for screening checked bags and ETDs are being used in place of EDSs for the time being.

Passengers with tickets and photo ID but no luggage to check can bypass the ticket counter (Johnson, 26 Mar 2002).

Figure 5.20. Invision's EDS at Chicago's O'Hare International Airport. (From: Johnson, 26 Mar 2002).

Lessons from abroad include (Masterson 3 Apr 2002):

- Government-trained security personnel interview all passengers at Ben Gurion International Airport for up to 20 minutes before they even get to the ticket counter (see Figure 5.21). Every passenger at Narita International Airport can also expect to be questioned before checking in. Experts are recommending that a similar model be used at U.S. airports.

Figure 5.21. Passenger Interviews at Gurion International Airport. (From: Masterson, 3 Apr 2002).

- Security officers at many European airports interview randomly selected passengers before allowing them to proceed to ticketing.

- Like many foreign airports, London's Heathrow International Airport (the largest in Europe) and the Hong Kong International Airport (Asia's largest) inspect all checked baggage.
- Airports in Europe and the Middle East employ baggage matching. No bags are loaded onto the plane until each passenger is onboard.
- In the wake of the attacks, some countries, such as Malaysia, are introducing biometric smart card in an attempt to strengthen their national security (Scheeres, 25 Sep 2001).
- Iris-recognition technology is being used to expedite the passport control process at Schipol Airport in Amsterdam, the Netherlands as part of a pilot program called the "Privium Project." In this program, iris templates and passenger details are stored on a smart card, and inserted into a reader when passengers pass through gates. Passengers are then required to look into a scanner, and their iris-developed template is compared to the iris template stored on the card. (Guevin, 9 Apr 2002)
- At Heathrow Airport in London, Virgin Atlantic Airways is using EyeTicket Corporation's JetStream iris recognition product line in a pilot program to expedite airline passenger processing at the passport control stage. JFK Airport in New York City and Dulles Airport in Washington, D.C. are also considering JetStream trials (Guevin, 9 Apr 2002).

Although six of the 9-11 hijackers were selected for special security screenings, two were singled out because of irregularities in their identification documents, and one was listed on ticket documents as traveling with one of the hijackers with questionable identification, all nine were able to successfully board their planes. Their checked baggage was checked for explosives or unauthorized weapons. They were able to board with their box cutters since such knifes were allowed on airplanes before 9-11 (Eggen, 2 Mar 2002).

4. Carry-On Baggage

To ensure detection of any weapons, metal detectors are set on the highest levels. Passengers are limited to one carry-on bag and one personal item. All bags may be subject to individual hand searches after screening (see Figure 5.22). Electronic items, such as laptop computers and cell phone may be subjected to additional screening. The same restrictions apply at foreign airports.

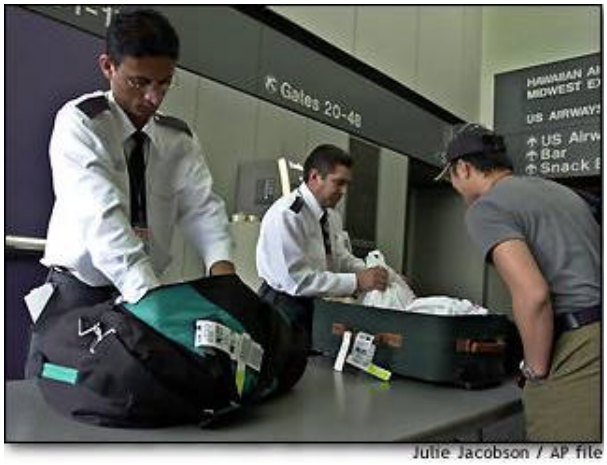


Figure 5.22. Physical Luggage Searches. (From: AP file, Julie Jacobson).

5. Security Checkpoints

At security checkpoints, biometric technologies, and video surveillance tools are being used to enhance the capabilities of an airport's CCTV system and the effectiveness of the security personnel. A new addition to developed biometric airport security systems is the National Integrated Security Suite, a collaboration of technologies from Identix, EDS, PwC Consulting, Sun Microsystems, and Oracle. The system is already deployed at Israel's Ben Gurion Airport and has processed about 1.5 million passengers since 1998 (see Figure 5.23). The suite includes:

- *Known Traveler* – a voluntary passenger registration system. Passengers can register using the Internet or at an airport kiosk by filling out a questionnaire and agreeing to a background check. Once cleared to be on the program, the registered passengers are directed to an airline affinity club, where they receive a smart card with an electronic template of their iris and fingerprint. This smart card is then used to expedite check-in by authenticating the "known" passengers.
- *Secure Employee* – pre-employment background investigations are issued for each potential airport employee or contractor. Each applicant is fingerprinted using Indentix Live Scan ten-print scanners (Guevin, 9 Apr 2002).

Figure 5.23. EDS's Known Traveler kiosk at Israel's Ben Gurion Airport. (From: Electronic Data Systems, 2002).

Since new, sophisticated non-metallic explosives designed to evade current explosive detection systems can be hidden inside shoes and belts or the frame of a carry-on bag, new scanners are being tested at airports. At Orlando International Airport in Florida, passengers can volunteer to go through security procedures designed to test a series of new devices the government is testing. One of the new technology products being tested, Rapiscan's Secure 1000 (see Figure 5.24), uses a weak x-ray technology similar to the body scanner that was discussed in Chapter IV. Another new technology being tested is Barringer Ionscan Sentinel sniffer, also discussed in Chapter IV (Masterson, 3 Apr 2002).

Figure 5.24. Rapiscan's Secure 1000. (From: Wilson, p. 53).

The Department of Energy's (DOE) Pacific Northwest National Laboratory is looking to employ holographic imaging technology called the 3-D Body Holo Scanner at airports and other locations. The scanner does not depend on ionizing radiation and can identify concealed weapons made of composite materials, plastic explosives, and liquids. The FAA funded the research project, and a prototype was built in 1992. The project stalled because the lab lacked a commercial partner to market and manufacture the scanners. The events of 9-11 have revived the interest in this type of technology and deployments of this technology are likely. SafeView is licensing the lab's holo-scanning technology. The technology is based on radar and an advanced computerized system that allows 3-D image reconstruction. The advantage of using radar waves is that they penetrate clothing but are reflected by skin and other objects hidden under clothing. The 3-D images are generated by measuring the time difference of the reflected waves that return to the detector. Algorithms are then used to illuminate concealed objects. Estimates on the initial costs for holo scanners are as high as $100,000 per unit (Paulson, 5 Aug 2002).

Lessons from abroad included (Masterson 3 Apr 2002):

- In addition to checking boarding passes and identification, airport personnel at Ben Gurion apply a security sticker to each passenger's boarding pass. The sticker prevents the passenger from re-entering the check-in area and is required during the boarding process.
- In several European and Asian countries, passengers can expect to be patted down if they set off the metal detector.

6. Waiting Areas

FAA agents are roaming airports with bomb-sniffing dogs. TSA security personnel are patrolling concourses, checking for unattended bags and watching for weapons. Lessons from abroad include:

- Armed guards patrol waiting areas of European and Asian airports.
- In addition to surveillance, Ben Gurion furnishes waiting areas with an eye toward passenger safety.

7. On-Board the Plane

The number of armed federal air marshals has increased since 9-11, giving top priority to nonstop, long-distance flights. Air marshals currently fly on select flights, including all flights in or out of Ronald Reagan Washington National Airport. Transponders, the devices that enable ground controllers to track a plane's flight path, can no longer be made inoperable from the cockpit.

The Transportation Department, with support from some in Congress, is considering video cameras that provide cockpit and cabin views (see Figure 5.25). United Airlines is conducting a six-month test of Rockwell Collins' cabin surveillance system. The system feeds images from as many as 32 cameras to hand-held computers in the cockpit (Wald, 30 May 2002).

Figure 5.25. Airplane Cockpit and Cabin Cameras. (From: Wald, 30 May 2002).

Images can also be beamed back into the cabin and picked up by pocket computers. This feature would allow air marshals to obtain the camera images using a PDA. The system can also be configured to record and play back the last few seconds, and can be set up to beam images of the cabin and cockpit to the ground. Honeywell is developing a similar system, which has fewer cameras but has infrared capability (Wald, 30 May 2002).

Animal surveillance is also playing an important role in ensuring that explosives are not being loaded into airplanes. When available, canines are being used to inspect airplanes and baggage (see Figure 5.26).

Figure 5.26. Animal Surveillance. (From: USA Today, 8 Feb 2002, Joel Salcido and Tyson, Jun 2002).

8. Ramp Access

The aviation regional hub system has millions of connections a year. However, bag matching is not required for connecting flights. This loophole led to the 1988 Pan Am bombing over Lockerbie, Scotland. A terrorist could gain access to the aircraft or baggage and slip explosives into the cargo bay, since they are not re-screened for the subsequent legs of their flights. Currently, there is no standard way of tracking lost ramp passes or ground crew identification. Therefore, many countries, including the United States, are investigating biometric smart cards as a solution (Masterson 3 Apr 2002). The Aviation and Transportation Security Act of 2001 calls for upgraded access control systems for secure areas at airports, and the best way to ensure that only authorized personnel gain access to secured areas is with the use of biometric technologies. The challenge will be to choose pick the best biometric technologies that fit the application.

9. Dangerous Goods

Items such as manicure sets, aerosol cans, and corkscrews are now considered possible weapons. These items are now required to be packed in checked-in luggage and are screened for at security checkpoints. Similar restrictions have been in place worldwide since the Sept. 11 attacks.

10. Employee Screening

Bombs can be slipped onto or carried aboard baggage handling equipment or can be left in bags at baggage claim. A would-be suicide attacker, using an acquired baggage-handling uniform, could load a deadly bag with others on a cart and move with little interference through a terminal. The Aviation and Transportation Security Act of 2001 mandates fingerprint background checks on all airline and airport employees.

The TSA now oversees aviation security rather than the airline industry and Federal Aviation Administration (FAA). By November, the TSA is scheduled to have its 30,000-strong workforce fully in place at more than 420 airports across the nation. The screeners will have to be U.S. citizens, fluent in English, with a background check and 100 hours of training under their belts. The FAA is piloting the use of smart cards in the Transportation Department by issuing cards to 50,000 FAA employees and contract workers (Vasishtha, p. 9). The new TSA is planning to use smart card authentication

system that use biometric identifiers such as fingerprints, iris scans, and encoded photographs to authenticate airline workers such as pilots and flight attendants (GCN, Jun 2002). Lockheed Martin Corporation has been contracted by TSA to integrate security at airports ($490 Million) and to train TSA employees in the techniques of screening airport passengers ($105 Million) (Hasson, 1 Jul 2002). Identix's live scan systems, which can be directly linked to the FBI IAFIS system, will be adopted by over 100 airports to aid in complying with the Aviation and Transportation Security Act of 2001 (Identix.com, 2002). Six Identix Live Scan TouchPrint 2000 Applicant Fingerprint Systems have been deployed in Chicago's O'Hare International Airport, the St. Petersburg-Clearwater International Airport in Florida, Lincoln Airport in Nebraska, Des Moines International Airport in Iowa, and Springfield Airport in Missouri (Guevin, 9 Apr 2002).

Lessons from abroad include (Masterson 3 Apr 2002):

- Employees at most foreign airports are required to be citizens of the country they work in.
- The Israeli government trains all baggage screeners at Ben Gurion International Airport. Japan requires 150 hours of classroom training for its baggage screeners. France requires 60 hours.

Information gathered from papers seized in Abu Zubaydah's hideaway in Faisalabad, Pakistan, included attacks on tankers and cruise ships (Reuters, 1 Jul 2002). Therefore, security at other transportation centers should not be overlooked. Security at cruise ship and bus terminals should also be strengthened. There is also a concern that terrorist could use some of the 200,000 general aviation aircraft (private planes) in the United States to carry explosives or scatter chemical and biological materials (Associated Press, 6 Jul 2002).

C. CRITICAL INFRASTRUCTURE PROTECTION

1. Terrorist Threat

Since al Qaeda will likely strike where they believe we are vulnerable, our cyberspace infrastructure is ripe for attack. Intelligence gathered from surveillances of chat rooms, interrogations of al Qaeda captives, and terrorist laptops found in Afghanistan and Pakistan have revealed al Qaeda's interest in conducting coordinated, conventional cyber attacks. One al Qaeda laptop found in Afghanistan had made

multiple visits to a French site (run by the Anonymous Society) that offers a "Sabotage Handbook" with sections on tools of the trade, planning a hit, switchgear and instrumentation, anti-surveillance methods, and advanced techniques. Computers in Islamic chat rooms linked to al Qaeda had access to cyber tools that can be used to search out networked computers, scan for security flaws, and exploit them to gain entry or full command. The most significant find by U.S. investigators was digitally logged evidence that al Qaeda operators had spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport, and communications grids (Gellman, 27 Jun 2002).

These unveiled and unsettling signs of al Qaeda's aims and skills in cyberspace mean that terrorists are at the threshold of using the Internet as a direct instrument for terrorism. Al Qaeda is suspected of having already tapped into some utility company computers in Northern California in an effort to find vulnerabilities. Unknown browsers originating from the Middle East and South Asia were detected conducting suspicious surveillance on digital systems that manage Bay Area utilities and government offices during the fall of 2001. The FBI, working with Lawrence Livermore National Laboratory, has traced trails of broader reconnaissance operations on various sites nationwide. The reconnaissance operations took place at the meeting points of computers and the physical structures they control. Routed through telecommunications switches in Saudi Arabia, Indonesia, and Pakistan, the browsers studied nuclear power plants, gas facilities, electrical generation and transmission, water storage and distribution, and emergency telephone systems. U.S. analysts believe that by disabling or taking command of nuclear power plant subsystems, of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to cause havoc in the real world, especially if it is conducted in conjunction with physical attacks. A conventional al Qaeda might be followed by cyber attacks to disrupt emergency first responders, fire mains, and power to hospitals (Gellman, 27 Jun 2002).

The risks of cyber-terrorism, until recently, were regarded as remote, but it is now commanding the attention of various government agencies. A security vulnerability in a data transmission standard Abstract Syntax Notification (ASN.1) discovered in February

2002 could have been exploited to bring down telephone networks and halt air traffic control communications. In a book-length Electricity Infrastructure Security Assessment, the industry concluded on 7 Jan 2002, "It may not be possible to provide sufficient security when using the Internet for power system control." To provide the needed security, power companies need to build a parallel private network for power system control. Digital control devices called distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems connected to the Internet can be exploited. These devices are used to collect measurements, throw railway switches, close circuit breakers, or adjust valves in the pipes that carry water, oil, and gas. Intruders have been able to assemble a detailed map of each system. They have also been able to intercept and change SCADA commands without detection (Gellman, 27 Jun 2002).

Two examples showing the vulnerabilities of SCADA systems include:

- In 1998, a 12-year-old hacker, exploring his cyber skills, broke into the computer system that runs Arizona's Roosevelt Dam. He did not know or care, but federal authorities said he had complete command of the SCADA system controlling the dam's massive floodgates.
- In Queensland, Australia, on 23 Apr 2000, police arrested Vitek Boden, 48, who had used commercially available equipment and software to turn his vehicle into a pirate command center for sewage treatment along Australia's Sunshine Coast. From his car, he remotely controlled 46 leakage events of hundreds of thousands of gallons of sewage into parks, rivers, and the grounds of a Hyatt Regency hotel (Gellman, 27 Jun 2002).

Nearly identical systems run oil utilities, gas utilities, and many manufacturing plants throughout the world. They are also used in the generation, transmission, and distribution of electrical power. To counter this threat, President Bush has launched a top-priority research program at the Livermore, Sandia, and Los Alamos labs to improve safeguards in the estimated 3 million SCADA systems in use. "Red Teams" of mock intruders from the Energy Department's four national laboratories have been able to devised eight scenarios for SCADA attack on an electrical power grid that work. Eighteen such exercises have been conducted to date against large regional utilities with alarming success (Gellman, 27 Jun 2002).

We can no longer ignore the amount of attention al Qaeda is paying to the Internet or underestimate their capabilities and ambitions. They have spent time mapping our

systems and vulnerabilities. In February 2002, the CIA issued a revised Directorate of Intelligence Memorandum, which stated that al Qaeda had "far more interest" in cyber-terrorism than previously believed and had contemplated the use of hackers for hire to speed the acquisition of capabilities (Gellman, 27 Jun 2002). To counter future reconnaissance operations, surveillance programs (ECHELON, Carnivore), cyber forensics and other tools, such as "honey pots," need to be used. EDS is offering a computer program that tracks cyber-attacks over time and shows any relationships among the attacks (Hasson, 1 Jul 2002). These tools could be invaluable tools to detect and gather intelligence on terrorist's future targets and actions. Biometric technologies should be used to control access to both public and private sensitive critical infrastructure networks. In June 2002, Sprint, one of two vendors on the General Services Administration (GSA) FTS 2001 telecommunications contract, added a number of products and services to preserve vital data and operational communications, such as video services and faster connections in the event of a catastrophic attack that knocked out communications (Hasson, 1 Jul 2002).

2. Recent Developments

Since 90 percent of the country's critical infrastructure is privately owned, government analysis and coordination is extending to the private sector. Legislation is being introduced to increase information sharing and threat analysis for critical infrastructure (CBSNews.com, 23 Jul 2002). To date there have been additional steps in protecting our critical infrastructure in this increasingly interconnected world (GCN, 24 Jun 2002):

- DOE's National Infrastructure Simulation and Analysis Center is collecting 10 years of research from Los Alamos and Sandia national laboratories' supercomputers to develop response plans to bio-terrorism, transportation, war games, economic consequence analysis, and infrastructure interdependency.
- GSA's Federal Computer Incident Response Center, working with Carnegie Mellon University's CERT Coordination Center, is studying a pilot program to use sensors in firewalls and intrusion detection systems to analyze intrusions and "hacks." Information will be collected government-wide and analyzed for trends. Initial pilot deployment will begin during Fall 2002 at four to five agencies with expansion nationwide within a year. GSA is also having a Request For Proposal (RFP) for

vendors to compile and market government-developed security tools to government agencies. The center also plans to develop a knowledge management portal that lets security managers access tools and services and communicate in a secure environment and link to a security patch Website that Science Applications International Corporation is developing.

- Justice Department's National Infrastructure Protection Center is developing:
  - Information Sharing and Analysis Centers to aid in identifying critical infrastructures such as water, financials services, transportation, health care, electric power, IT, and telecommunications, and provide threat assessments on each.
  - Data Mining and Data Analysis Project to be able to retrieve real-time incident data from multiple, analyze the data, and generate incident reports.
  - A large government-industry partnership to share information about system intrusions and other critical infrastructure protection.
  - A Key Asset Initiative to prepare a comprehensive database of critical infrastructure assets in the United States. The database would identify and protect information on more than 5,700 entities vital to national security to protect critical infrastructure against physical and cyber-attacks.

D. FINANCE

1. Financial Surveillance to Detect Terrorist Funding

Some of the nation's largest banks are installing new software products, which can screen new and current clients for potential terrorist ties. The software can also examine millions of daily transactions for suspicious patterns of behavior, such as indications of money laundering and terrorist funding. Using the Treasury Department's secure online Financial Crimes Enforcement Network (FinCEN), financial institutions can report any suspicious account activity or customer behavior. As of 5 Jun 2002, suspected terrorists' assets totaling more than $115 million have been frozen worldwide (Barrett, 12 Jun 2002).

E. HEALTH CARE

1. Health Care Information Systems

Given that the outbreak of disease may now be the result of deliberate and widespread attempts to infect rather than natural spread of infection, government and

health experts have recognized a need for rapid (near-real time) surveillance and detection of disease. This has led many universities and hospitals to develop systems to collect and analyze disease data immediately at hospitals and emergency rooms as a patient is admitted:

- A system called Real-Time Outbreak and Disease Surveillance (RODS), financed by the National Library of Medicine, is being developed at the Center for Biomedical Informatics at the University of Pittsburgh. It receives patient information, such as patient's chief complaint, reported health problems, patient's age, time, and date of visit, gender, and ZIP Code. Personal information, such as name, address, and social security number is not shared to protect privacy. The information is obtained as soon as the patients are admitted, through a private computer network from 15 Western Pennsylvania hospital emergency departments. The system looks for similarities between new reports with those already stored in the central database, and uses geographic information software to reveal any geographical patterns behind the surveillance information. To aid in detecting any incidents of bio-terrorism during the Winter Olympics in Salt Lake City in February 2002, RODS was used to connect 30 area hospitals and walk-in clinics. Based on the number of patients who showed up with respiratory complaints during this period, the system was able to detect an influenza outbreak (Greenman, 4 Jul 2002).
- Children's Hospital Project in Boston, financed by the federal Department of Health and Human Services, is another real-time surveillance program that is being developed. It monitors complaints at Children's Hospital and neighboring Beth Israel Deaconess Medical Center. Several area hospitals are expected to participate in the project in the coming year (Greenman, 4 Jul 2002).
- The New York City Health Department has a medical early warning system, which links emergency rooms, 911 dispatch facilities, and pharmacies throughout the city (Walsh, p. 16).
- The Centers for Disease Control and Prevention's Health Alert Network (HAN), a secure e-mail and fax alert system, is being considered as the basis for a national medical intelligence database (Walsh, p. 1).
- The Department of Health and Human Services (HHS) is developing Metropolitan Medical Response Systems (MMRS) to enable cities to coordinate emergency first responders, public health systems and hospitals to better respond to the needs of the community during a crisis situation (HHS News, 10 Jul 2002).

2. Wireless Priority Access Service

To give first responders and other emergency preparedness officials priority access to wireless service during disasters, a DOD's National Communications System has been running since April 2002 in New York City and Washington D.C. VoiceStream is the program's carrier, and plans are to expand the program nationwide (GCN, Jun 2002).

3. Information Security

To meet recent government legislation surrounding the integrity, confidentiality, and privacy data of patient data, the healthcare industry is restructuring current IT infrastructure and methods. Biometric technologies are being used to implement security mechanisms to secure stored or in-transit patient confidential information, to protect against disclosure of patient data, and to enable only authorized personnel to view patient records (Indentix, 2002).

4. Physical Security

Biometric technologies are being employed or are being considered for use at many hospitals and laboratories that contain hazardous chemicals or materials. These systems also allow for audit and positive ID of individuals who enter and exit these areas.

F. LAW ENFORCEMENT AND INTELLIGENCE

1. Criminal Background Checks

A bigger challenge than settling on a specific biometric identifier is putting together an enterprise-wide system for storing, accessing, and retrieving biometric templates in a timely matter. The Federal Bureau of Investigation has been developing a nationwide digital data network in order to determine the identification of individuals and to match it with records already on file. This network will provide quick access to a new integrated Automated Fingerprint Identification System (AFIS) and will speed up suspect identification (I/O Software, Jun 2002). A similar network is also being considered in the U.S. for children fingerprints in order to identify a child (whose identity might have been changed after abduction) by comparing the fingerprints against a national database of missing children's fingerprints (Polemi, p. 33).

2. Mugshot/Booking Systems

Imagis Technologies and ORION Scientific Systems are collaborating in an effort to deploy a digital image network based on Imagis' ID-2000 facial-recognition software and its centralized digital booking system called the Computerized Arrest and Booking System (CABS). All enrolled digital facial images and suspect information is stored in the system's shared database. The data store in the centralized database can be accessed at any time and from any location (Guevin, April 9, 2002).

3. Mobile Identification

Identix has patented wireless identification systems that use fingerprints and/or photographs and allow police officers to access criminal databases. These systems could be configured to link with FBI and CIA watch lists to catch any suspected terrorist who may be stopped for a traffic violation.

Identix's IBIS system (see Figure 5.10 above) is being employed at the West Valley city police department near Salt Lake City, UT. The IBIS system will interface with legacy law enforcement databases. It will enable field officers to capture forensic-quality fingerprints and facial images on handheld devices and submit them through a cellular connection. The objective is to compare and match against criminal and fugitive records in AFIS and other available systems. If a match is not made, the files are discarded from the system. The police department is using six mobile units with the IBIS server residing with the Ontario police department in California. West Valley's criminal fingerprint files and criminal files have been added to the server in California and will be wirelessly accessed (Guevin, April 9, 2002).

Visionics Corporation's IBIS mobile identification system is being installed at Hennepin County sheriff's office in Minnesota, and the Redlands, California police department. A handheld Remote Data Terminal is used to capture photographs and forensic-quality fingerprint images or magnetic stripe data. The information is first transmitted wirelessly to a laptop in the squad car. It is then transmitted to a central IBIS server through the police radio communication system or via cellular communications. Once the information has reached the central server, it is processed and transferred to one or more AFIS databases for fingerprint matching. Positive matches alert the Remote

Data Terminal. If there is no match, fingerprint and photo files are discarded (Guevin, April 9, 2002).

4. Facial Surveillance

More and more law enforcement departments across the country are lobbying their city and state legislatures to use facial recognition surveillance technologies. An example is the Virginia Beach Police Department, which is installing Identix Corporation's facial recognition system with 13 CCTV cameras that will monitor the beach area for criminals, missing persons, and runaways (CardTechnology.com, 3 Jul 2002).

5. Electronic Surveillance

As the U.S. and its allies continue to hunt down terrorist cells throughout the world, al Qaeda, Hamas, Hezbollah, and other militant Muslim groups are increasingly turning to the Internet to raise funds, recruit, and coordinate their activities. The FBI, CIA and other agencies need to continue to search e-mail traffic for specific senders, recipients, and keywords. They must monitor the Web for rouge websites, such as Jihadunspun.net, Azzam.com, Alneda.com, Almuhajiroun.com, and Qassam.net. The challenge facing agencies is that most of the information on these websites is written in Arabic, encrypted, and hidden in digital photographs. The militant groups also regularly change the addresses of their websites to hinder intelligence surveillance efforts. They use computers in libraries and cyber cafes (Kelley, 10 Jul 2002). Systems such as Echelon and Carnivore can aid in electronic surveillance efforts. Magic Lantern can aid in recording keystrokes on targeted computers at these locations, thus circumventing encryption (O'Hanlon, Summer 2002).

6. Information Systems

The problem facing federal agencies is not that there is not enough information or intelligence. It is that they have too much and have not fully integrated effective repositories of data that can be shared. Intelligence agencies also do not have enough interpreters and analyzers to look at the vast amount of information in a timely matter. "Actionable" intelligence is what is needed for the CIA, FBI, and NSA to compile the current daily picture of terrorist threats. According to FBI Director Robert S. Mueller III,

> It would be nice if…you put into our computer system a request for anything relating to flight schools, for instance, and have every report in the last 10 years that…mentions flight schools or flight training and the like kicked out…We do not have the capability now…We have to have that capability. (Miller, 13 Jun 2002)

To detect terrorist operations before they occur, U.S. agencies must use information effectively—collecting, collating, analyzing, sharing, and then deploying it quickly and in a useful form. Although considerable resources have gone to ensure that these tasks were conducted prior to 9-11, serious weaknesses exist that must be addressed. Prior to 9-11, information strategy lacked an overall architecture. The need for strong human intelligence assets was somewhat ignored. Massive amounts of information was available but was of little value because it was not analyzed promptly due to lack of translators or was not shared in a useful way. In addition, agencies did not collate and promptly combine raw shared data to develop a meaningful picture. To correct some of these weaknesses both the public and private sectors are improving their abilities to collect and analyze data with the use of collaborative tools and data mining agents.

a. Information Management and Database Issues

The federal government has more than a dozen terrorist watch lists and at least 55 databases, which contain watch list information. However, two of the 9-11 hijackers were on a CIA watch list, but the airlines had no access to government databases that would have alerted them of the two men (Miller, 13 Jun 2002). The truth is that the FBI and the other government departments and agencies have an uneven blend of antiquated computer systems that require upgrading. The FBI has over 35 separate investigative database applications that they use (Miller, 13 Jun 2002). Component agencies, such as the Secret Service, has a mix of Windows, Unix, and Linux platforms, plus multiple vendors' database management systems and telecommunication platforms. FEMA and the Coast Guard run mostly Microsoft Windows NT environments that require near-term upgrade because of NT's phase-out. In contrast, the Border Patrol has a secure intranet and a centralized Oracle database. Most federal law enforcement databases cannot communicate with each other. Local and state databases also cannot link and share information with federal, state or local agencies.

Fixing information management and database issues are the corner stones of President Bush's proposal to create the new Homeland Security Department that, using his words, "will review intelligence and law enforcement information from all agencies of government and produce a single daily picture of threats against our homeland (Miller, 13 Jun 2002)." Almost every new federal initiative for homeland security has involved an increase on storage, with a particular emphasis on the management of large information databases. Agencies are exploring more efficient ways to manage the increasing volumes of data and to make it accessible throughout the new Homeland Security Department and associated agencies.

President George W. Bush's Homeland Security proposal calls for a single enterprise architecture to eliminate duplication (Menke, p. 1). Seat management and outsourcing are emerging as the keys to transforming the systems of seven dissimilar agencies into the enterprise architecture that is envisioned by the President: the Immigration and Naturalization Service (INS); the Secret Service; the Customs Service; the Animal, Plant, and Health Inspection Service (APHIS); the Coast Guard; the Federal Emergency Management Agency (FEMA); and the Transportation Security Administration (TSA). Some agencies, such as the INS, have taken steps in this direction. Other agencies, such as the Customs Service and the Secret Service, which have built their IT environments piecemeal, will have more difficulty going in this direction (Menke, p. 12).

Once established, the new unified enterprise architecture will become the first large-scale test of the Office of Management and Budget's initiative to unify and simplify government systems (Menke, p. 1). The biggest challenge facing the Homeland Security Department is determining how to set up its databases. Choices include the development of a multi-terabyte data warehouse, enable streaming of multiple data sources through a Web portal interface, or enable querying of the component agencies' existing databases (Menke, p. 1). The new enterprise architecture must accommodate disparate databases and legacy applications, linking communities within and outside government via standards-based technology (Jackson, p. 12).

b. Counter-Terrorism Information Technology (CTIT)

Technology exists to link existing databases or to create new databases that can be mindful of privacy and constitutional concerns (Miller, 13 Jun 2002). As an example, software similar to that used by credit card companies could be used to track the movements of suspected terrorists by tracking their credit card purchases, residences, and communications. The Independent Task Force on America's Response to Terrorism of the Council on Foreign Relations proposed a Counter-Terrorism Information Technology (CTIT) system that uses commercially available techniques from the private sector, including database merge-and-search techniques that are currently used by many Internet applications (Lodal, 1 Apr 2002). The commercial sector has already developed and fielded many applications that integrate vast amounts of information from multiple data points, scan this information based on "suspicion rules," and generate rapid alerts based on set parameters. CTIT can be directly translated from the existing civilian applications (see Table 5.2):

Technique	Commercial Application	Counter-Terrorism Application
Touchpoints	Web site visit, call center, point of sale, customer service call	Visa interview, border crossing, school registration, ticket purchase
Information Captured	Web click, items bought, quality complaint to customer service	Visa type, border location, school name, ticket destination, date, and class
Data maintained	Internet service provider, on-line account activity, store purchased items	Current residence, educational courses, travel routes and frequency
XYZ relationships identified	Credit card X owned by internet ID holder Y who shops as buyer Z	Visa holder X attending school as student Y traveling as credit card holder Z
Pattern alert rule	If customer XYZ has higher than average on-line purchases of video equipment and has claimed more than 2 cash refunds at multiple stores within 24 hours, and is standing at a customer service return desk with another video camera return, page a security guard.	If foreign student XYZ has missed more than 2 weeks of aviation class and has used a new credit card to book more than 2 plane trips to the same city in 1st class, email the school and the district FBI office.

Table 5.2. Translation of CTIT from Existing Civilian Applications. (From: Lodal, 1 Apr 2002).

These applications can be leveraged to enable government agencies to track, address, and prevent terrorist activities (Lodal, 1 Apr 2002). A system that uses the CTIT model (see Figure 5.27) could bring together members of the various federal, state, and local communities to address the effects of information sharing on homeland security. It would meet the objectives of gathering, sharing, interpreting, and presenting information across the intelligence and law enforcement communities at federal, state, and local levels.

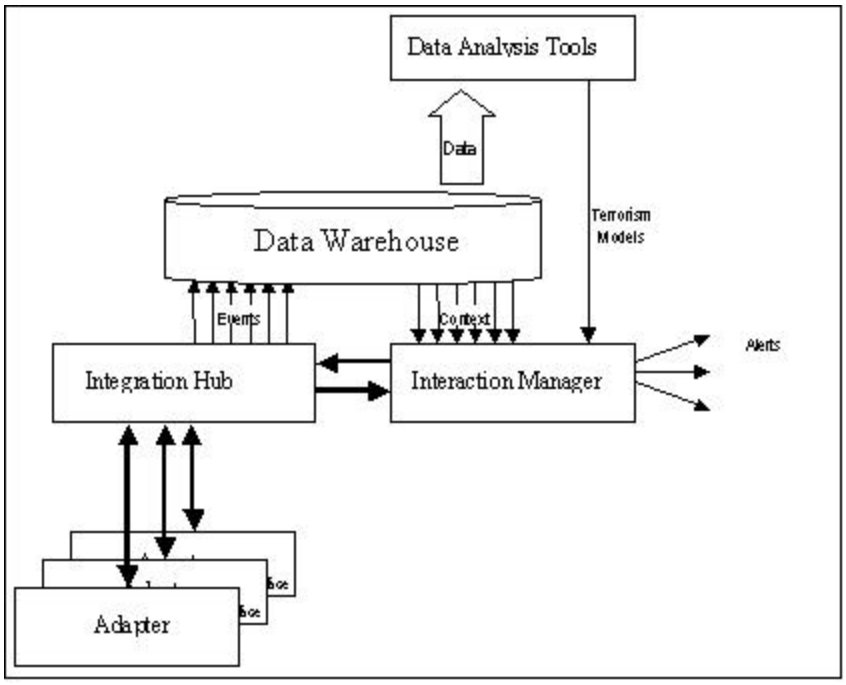


Figure 5.27. Architecture of the CTIT. (From: Lodal, 1 Apr 2002).

The major components of the CTIT solution are (Lodal, 1 Apr 2002):

- *Adapter module* – provides the means for agencies and civilian agents to give periodic data or information, and to forward messages presenting interesting events to the CTIT environment, in a common data format such as XML.
- *Integration Hub* - provides the ability to log, route, transform messages from the Adapters, and calls on the Interaction Manager to evaluate events in real time and inserts the events into the real time data store.

- *Data Warehouse* – provides real time, integrated data store of events from all participating agencies and organizations.
- *Analytic Engines* – use data-mining software to analyze CTIT data and develop models. Models of high-risk scenarios are constructed of events and their surrounding context. Multiple analytic environments are maintained to support various organizations that have access to the Data Warehouse.
- *Interaction Manager* – uses an inference based rules engine to evaluate events as they occur and executes data-mining modules against context data within the Data Warehouse, as well as current event data. It issues alerts to specific client groups in the event of suspicious outcomes and high-risk events.

c. Other Developments

There have been several recent developments within the law enforcement and intelligence communities to address data mining, collaboration, and information sharing:

- EDS and Public Safety Systems are collaborating to develop a product called Ramsafe, which can provide virtual blueprints of buildings for SWAT teams in hostage situations. It will also be able to analyze biological or chemical attack scenarios, how many people are likely to be affected, and provide the location of the nearest hospitals (Hasson, 1 Jul 2002).
- National Infrastructure Simulation and Analysis Center, in conjunction with Los Alamos National Laboratory and Sandia National Laboratories, is developing intelligence assessment tools that include high-end modeling software (Menke, p. 12).
- Currently, a client-server system, called GENOA, is being used by agencies to collaborate and share information on issues relating to Homeland Security.
- As one of the first to steps taken to begin the reorganization and revamping of government systems, the Office of Homeland Security identified databases from federal departments and agencies to determine which have information pertaining to areas such as border control, bio-terrorism prevention, and emergency response (Miller, 13 Jun 2002).
- The FBI and CIA are providing airlines with "no-fly" lists of suspected terrorists.
- Lately, al Qaeda has stressed the use of encrypted email messages, and websites, some of which were being hosted from locations in the tribal

areas of Pakistan. This has made it even more important for agencies to develop and use electronic surveillance tools. (Gunaratna, p. 35)

- Problems still persist on "names" of suspected terrorists in current watch lists (Diamond, 1 Jul 2002):
  - Variations in spelling of an Arab name.
  - Conflicting methods are used by agencies to translate and spell the same name.
  - Antiquated computer software applications at some agencies do not allow searches for approximate spelling of names.
  - Large volume searches result from common Arabic names, such as Muhammed, Shiek, Atef, Atta, al-Haji and al-Ghamdi.
  - Some names in databases are just nicknames and not family names.

This problem could be addressed, however by using biometric templates (if available) as part of the watch-list database.

Privacy watchers are monitoring all biometric and surveillance developments closely, concerned for possible abuses as government may seek to tap into private databases containing credit data, health information, travel records, and other personal data, along with video from private surveillance systems. These concerns are being heightened by new FBI guidelines that will permit agents to more freely conduct surveillance at political rallies and religious gatherings, surf the Internet, and mine commercial databases for information (Miller, 13 Jun 2002). However, in this new war all tools are needed since the old rules provided terrorist with a "competitive advantage." As Dr. John Arquilla, Associate Professor for the Department of Defense Analysis at Naval Postgraduate School has stated, "our adversaries have learned to 'ride the rails' of our advanced technology, and our free ways, to strike us." (Arquilla, 4 Apr 2002). It is now time for us to make it more difficult for them to maneuver, plan, and execute further attacks by implementing advanced surveillance and biometric tools. As al Qaeda continues to seek new alliances with other extremist groups in order to create "super cells," our biggest challenge is and will continue to be targeting information flows. It is paramount to continue to listen to communications to acquire intelligence and warnings.

Rouge states may be reaching out to terrorist networks (Arquilla, p. 352). These rouge states can actively harbor, finance, and nurture these networked terrorists.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. PRIVACY, SOCIETAL ISSUES, AND EMERGING LEGISLATION

A. THE HARD NEW REALITIES

The research presented in this chapter will speak to the evolving social discussions, initiatives, and legislation concerning employment of surveillance, biometric recognition and other tracking/profiling technologies. Though the privacy hardliners have been crying foul for some time about "Big Brother" eroding our civil liberties, we are increasingly beginning to see that ubiquitous surveillance and biometric technologies may very well be the answer to actually protecting and preserving our rights—the right to safety and security in a growingly hostile world. September 11th completely changed the way we view the world. One of the findings is that people are far less concerned about what the private sector is doing with information and far more concerned about what the government is doing to keep them safe (Delio, 8 Nov 2001). The following Harris Poll taken in late September 2001, Table 6.1, reflects public sentiment that law enforcement's use of surveillance is finding more acceptance even as it affects some civil liberties.

There should not be any doubt among the general population that, even before the terrorist attacks of 9-11, we have been subjected to surveillance in public places in our daily lives. Surveillance has become a necessary presence in a society whose population is increasing—and with it, the rise of crime, and other unlawful activities. One can argue that the monitoring of citizens is a necessary invasion of privacy for the sake of safety and preservation of good order in society. Though we are not under constant surveillance yet in public, people can anticipate the day where every area of public life from work, to shopping, to commuting and leisure activities may be under surveillance. It is a natural reaction for people to feel that their civil liberties are being threatened. The CEO of Sun Microsystems, Scott McNealy, told reporters in 1999, "You already have zero privacy. Get over it" (Amato, p. 60). By mere observation, we have to assume he is correct. The numerous cameras in operation today monitor financial business areas, ATMs, department stores, parking lots, buildings, access points, highways, railways, and

bridges—one can think of a myriad of places a camera may be watching. And those are just the cameras that you can see.

Civil liberties vs. law enforcement

Here are some increased powers of investigation that law enforcement agencies might use when dealing with people suspected of terrorist activity, which would also affect our civil liberties. The Harris Poll asked 1,012 adults to approve or disapprove of each proposal.

	Favor	Oppose	Not sure / Declined
Expanded under-cover activities to penetrate groups under suspicion	93%	5%	1%
Stronger document and physical security checks for travelers	93%	6%	1%
Stronger document and physical security checks for access to government and private office buildings	92%	7%	1%
Use of facial-recognition technology to scan for suspected terrorists at various locations and public events	86%	11%	2%
Issuance of a secure I.D. technique for persons to access government and business computer systems, to avoid disruptions	84%	11%	4%
Closer monitoring of banking and credit card transactions, to trace funding sources	81%	17%	2%
Adoption of a national I.D. system for all U.S. citizens	68%	28%	4%
Expanded camera surveillance on streets and in public places	63%	35%	2%
Law enforcement monitoring of Internet discussions in chat rooms and other forums	63%	32%	5%
Expanded government monitoring of cell phones and email, to intercept communications	54%	41%	4%

Table 6.1. Harris Poll on Surveillance Use in Law Enforcement. (From: Sullivan, 14 Nov 2001).

There is no finer example today of a society under surveillance than the United Kingdom, which has nearly 2.5 million closed circuit television (CCTV) cameras installed; more per capita than any other nation (Big Brother, 13 Aug 2001). Never in history has any nation pursued ubiquitous surveillance to such an extent as the UK. Closed circuit cameras dot the nation like a spider web of watchful eyes, keeping vigilance over an active populous. The growth has been so profound that the network has been dubbed as "the fifth utility" —joining gas, water, electric and telephone (Amato, p. 59). This public surveillance project began in 1986 on an industrial estate near the town

of King's Lynn, approximately 100 kilometers north of London. Prior to the installation of three video cameras, a total of 58 crimes had been reported on the estate. None was reported over the next two years. The U.K. Home Office, the government department responsible for internal affairs in England and Wales, is starting construction of what promises to be the world's biggest road and vehicle surveillance network, a comprehensive system of cameras, vehicle and driver databases, and microwave and phone-based communications links that will be able to identify and track the movements of vehicles nearly nationwide (Amato, p. 59). In 1999, 500 British towns and cities had public CCTV systems installed, up from 74 in 1996 (Graham, Issue 3, 2000). Britain is thick with surveillance infrastructure; it has become a ubiquitous network that is all too often taken for granted (Graham, Issue 3, 2000). The trend for monitoring and surveillance is only increasing, especially in light of new world concerns in combating terrorism and preventing the use of weapons of mass destruction. So it is natural to see statistics that reflect people being willing to sacrifice some of there privacy in trade for more safety and security. You only need to be a victim of crime or a personal attack once to see the benefits of prevention, detection, and early notification, which surveillance can bring. British CCTV surveillance is now quickly spreading from main towns and cities to smaller and more remote rural areas, primarily because of citizen concerns of crime overspill from the more populous urban areas (Graham, Issue 3, 2000). Another catalyst for the spread of surveillance has been the natural linkage between CCTV, television news, and reality TV programming. Programs such as "America's Dumbest Criminals," "Caught on Tape," and "Police Stop!" have created "near entertainment" as the public is witness to individuals caught in the act of a crime (Graham, Issue 3, 2000). The social and psychological commentary is profound. Viewers of such surveillance programs react by developing further anxieties about the risks of crime and subsequently are likely to support the expansion of surveillance networks, spiraling the urgency for more surveillance. British sociologists are discovering that the more murders, terrorist acts, and other crimes are captured by CCTV, the greater the demand for surveillance in the society; a process sociologists call "normalization" (Graham, Issue 3, 2000).

As surveillance and biometrics technology becomes more sophisticated and evolves, we are now seeing the introduction of cross-checking of individuals' video imagery against motor vehicle databases, licensed drivers databases, most wanted lists, and other law enforcement and business transaction databases. The technology of biometrics in surveillance can distinguish faces, voices, irises, fingerprints, and other bodily identifiers. Improved intelligent software working within the surveillance systems can infer possible intent and alert authorities of need be. The message is a powerful one—the more surveillance in society, whether justified or not, the more potential there is to track and document everyone's behavior.

Hence, the systems that watch over us might be interpreted by some as an invasion of privacy, an infringement of civil liberties, or perhaps it may be called—the greatest invention to come for enabling law enforcement, keeping good public order, and improving safety. Societal positions for, or against surveillance may differ depending on what side of the law you are on, or if you have something to hide, or if you merely disagree on principle. One thing is for certain, surveillance is here to stay—terrorism and the proliferation of weapons of mass destruction (WMD) have solidified the arguments for surveillance as a necessity for the greater good of civilization.

There is no question that surveillance technologies can also be misused like any other technology, and people can become victims of the very system that was designed to protect them. Ethics, policy, law, and the will of the people are influencing the direction we are heading. Hammers were not outlawed the first time a crime was committed with one, nor will we see surveillance technology depart the stage when someone uses it improperly. That is why this technology is so controversial; we need standards, sound and balanced laws, and effective use policies to protect the rights of law-abiding people. We also need clear guidance to effectively use surveillance and biometric technology to detect illicit activities and apprehend criminal elements in society, while simultaneously keeping the process of surveillance unobtrusive and preserving the freedoms of a civilized nation. This is a tall order, but like any endeavor, it must begin with the presentation of all sides of the argument in pursuit of a balanced middle ground.

B. PRESENT DAY PRIVACY LAW

In a recent industry survey on electronic monitoring and surveillance, more than three-quarters of U.S. firms revealed that they monitor their employees' phone calls, e-mails, Internet activities, and computer files (AMA, 2002). The expectation of privacy in public and in the workplace has dimensioned as government, law enforcement, and businesses battle to reduce crime, fraud, waste, and abuse. Governments and businesses are justifiably concerned with maintaining productivity, reducing waste, preventing theft, espionage, and avoiding liability for the actions of employees. The courts have more often favored the interests of business and government than the privacy rights of the general public, thus reflecting the reality of federal laws. One of the few exceptions to this trend is the Employee Polygraph Protection Act of 1988, which bars polygraph testing except for certain cases of unique circumstances (Doyle, 1999). Many scientists consider polygraph testing to be untrustworthy, yet it has been used as the basis for employee dismissal (Doyle, 1999).

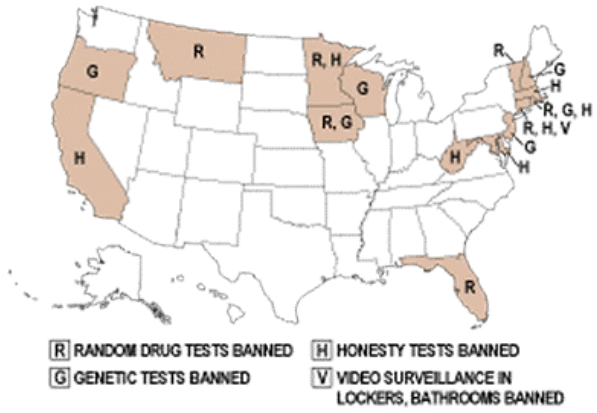


Figure 6.1. Privacy in the Workplace. (From: Doyle, 1999).

Some states have taken it upon themselves to compensate for shortcomings in federal privacy law by enacting state laws that provide greater protection of rights. Although federal law takes precedence, employers are typically subject to both state and federal laws. The map on Figure 6.1 shows states that ban various activities including paper-and-pencil honesty tests, which have not been scientifically validated (Doyle, 1999). No state gives strong privacy protection to workers using e-mail, voice mail, or

the telephone, nor does any state prohibit intrusive psychological testing (Doyle, 1999). The map illustrates that state laws provide only spotty overall support for worker privacy. Surprisingly, it also shows that worker protection from state laws is weak in the seven states stretching from New York to Missouri, where unions are strongest (Doyle, 1999). One might infer by this that Unions as well employers have desires for keeping the public work-pool clean of illicit conduct or activity. The impact of illicit conduct on safety, morale, and the bottom line are too great to ignore.

Surprisingly, the Constitution of the United States makes no assurances that people have an "absolute expectation" to privacy. The Fourth Amendment of the Constitution, which addresses privacy in terms of search and seizure, gives support to law enforcement authorities when there is reasonable suspicion of criminal activity involving the individual or their property, or compelling government interest to examine the individual more closely. Although each case is treated individually based on its own unique circumstances, under the guise of reasonable suspicion, the law heavily favors the authorities, the safety of law enforcement personnel, as well as good public order (Senate Document No. 106-27). For example, an individual driving a car on a public road has no reasonable expectation of privacy while he is driving from one place to another. The logic follows that when on public roads, people voluntarily convey to anyone who wants to look, the fact that they are traveling over a particular road, and when they exit and pull into a private driveway, they reveal publicly their final destination. Hence, for the most part, law enforcement authorities are within the law to use video surveillance on public roads. On the other hand, if video surveillance used by police has an infrared device with the capability to observe activities that a reasonable person might expect to not see from public view, Fourth Amendment concerns might surface (Nieto, June 1997).

C. EMERGING LAW

The laws to govern and manage surveillance and biometric technology are still evolving. The use of this technology is more likely than not to be controversial, primarily because we are so sensitive as a nation accustomed to maintaining our freedom, privacy, and civil liberties. America may have to turn to some of its more experienced international neighbors such as the UK, for guidance in implementation.

Our government's initial responses to the terrorist attacks of September 11th were several pieces of legislation that provide sweeping powers for surveillance and information collecting authority. The following are just a sampling of recent legislation related to development and deployment of technology solutions for improving security for the homeland:

1. Committee on Homeland Security and Terrorism

Senator Pat Roberts of Kansas sponsored the establishment of a Select Committee on Homeland Security and Terrorism. This legislation provides the committee to make regular and periodic reports to the Senate on the nature and extent of the homeland security and antiterrorism activities of the various departments and agencies of the United States, and review the activities of the agencies or departments concerned with the detection, deterrence, and management of the consequences of terrorism and incidents of terrorism in the United States (ANSER, S.R.165, 2002).

2. Department of National Homeland Security Act of 2001

Senator Joseph Lieberman of Connecticut sponsored the Department of National Homeland Security Act of 2001. This legislation provides for the establishment of the Department of National Homeland Security to (1) plan, coordinate, and integrate those United States Government activities relating to homeland security, including border security and emergency preparedness, and to act as a focal point regarding natural and manmade crises and emergency planning; (2) to work with State and local governments and executive agencies in protecting United States homeland security, and to support State officials through the use of regional offices around the Nation; (3) to provide overall planning guidance to executive agencies regarding United States homeland security; (4) to conduct exercise and training programs for employees of the Department and establish effective command and control procedures for the full range of potential contingencies regarding United States homeland security, including contingencies that require the substantial support of military assets (ANSER, S.1534, 2002).

3. The Airport and Seaport Terrorism Prevention Act

Senator John Edwards of North Carolina sponsored the Airport and Seaport Terrorism Prevention Act. This legislation provides for consultation with the United States Coast Guard and the United States Customs Service, in providing grants for

seaport security infrastructure improvements for an eligible project at any United States seaport involved in international trade. Eligible projects would be those involving construction, acquisition, or deployment of surveillance equipment and technology, including— (1) surveillance cameras with video feed to regional and national offices of the United States Customs Service that provide real-time information, observation, and situation status; (2) a pilot program for iris recognition or similar biometric technology for port workers with access to secure areas; (3) x-ray, ultrasound, and laser scanners to scan cargo containers; and (4) radiation monitors and other devices capable of detecting weapons of mass destruction, including chemical, biological, or similar substances (ANSER, S.1429, 2002).

4. Aviation and Transportation Security Act

Senator Ernest F. Hollings of South Carolina sponsored the Aviation and Transportation Security Act. This legislation provides for (1) short-term assessment and long-term deployment of emerging security technologies and procedures to prevent access to secure airport areas by unauthorized persons; (2) review of the effectiveness of biometrics systems currently in use at several United States airports; (3) review of the effectiveness of increased surveillance at access points, (4) review of computer-assisted passenger prescreening systems for evaluating all passengers and their luggage, (5) additional appropriations for research and development of aviation security technology for FY 2002-2006; (6) acceleration of research, development, testing, and evaluation of explosives and weapons detection technology for checked baggage, carry-on baggage, cargo, catered materials, and duty-free items; (7) and acceleration of research, development, testing and evaluation of integrated systems of airport security enhancement, including quantitative methods of assessing security factors at airports selected for testing such systems (ANSER, S.1447, 2002).

5. Uniting and Strengthening America Act (USA Patriot Act of 2001)

Senator Tom Daschle of South Dakota sponsored the Uniting and Strengthening America Act (USA Patriot Act of 2001). This legislation provides for strengthening America domestically against terrorism through (1) enhanced surveillance procedures and authority to intercept wire, oral, and electronic communications; (2) authority to share criminal investigative information; (3) increased information sharing for critical

infrastructure protection; (4) review of the integrated automated fingerprint identification system for points of entry and overseas consular posts; (5) improvements to US border protection; (6) removing obstacles to investigating terrorism; (7) improving intelligence; (8) and strengthening criminal laws on terrorism (ANSER, S.1510, 2002).

6. The Port and Maritime Security Act of 2001

Senator Ernest F. Hollings of South Carolina sponsored the Port and Maritime Security Act of 2001. This legislation provides for better methods of communication amongst law enforcement officials responsible for seaport boundary, security, and trade issues. It formulates guidance for the review of physical seaport security, recognizing the different character and nature of United States seaports. Eligible projects would be those involving construction, acquisition, or deployment of surveillance equipment and technology, including— (1) equipment or facilities to be used for seaport security monitoring and recording; (2) security gates and fencing; (3) security-related lighting systems; (4) remote surveillance systems; (5) concealed video systems; or (6) other security infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers. (ANSER, S.1214, 2002).

7. Chemical Security Act of 2001

Senator Jon Corzine of New Jersey sponsored the Chemical Security Act of 2001. This legislation provides for help in protecting the public against the threat of chemical attacks, and accidental or criminal chemical release (ANSER, S.1602, 2002).

8. State Bioterrorism Preparedness Act

Senator Evan Bayh of Indiana sponsored the State Bioterrorism Preparedness Act. This legislation provides for enhancing domestic preparedness by developing a national bioterrorism surveillance and detection capacity, developing and distributing rapid and more reliable diagnostic capabilities and systems, developing a comprehensive strategy for assuring surge capacity for health care, streamlining national pharmaceutical stockpiling efforts, and increasing research and development for new pharmaceuticals, vaccines and antidotes are essential endeavors (ANSER, S.1520, 2002).

9. Bioterrorism Preparedness Act of 2001

Senator Bill Frist of Tennessee sponsored the Bioterrorism Preparedness Act of 2001. This legislation provides for the ability of the United States to (1) improve

surveillance, detection, and response activities to prepare for emergency response activities including biological threats or attacks; (2) carry out activities to improve communications and coordination efforts between healthcare and federal government entities, including activities to improve information technology and communications equipment available to health care and public health officials for use in responding to a biological threat or attack or other public health emergency and including early warning and surveillance networks that use advanced information technology to provide early detection of biological threats or attacks; (3) improve animal, plant and food product surveillance at domestic and international ports and customs; (4) enhance methods of protecting against the introduction of plant and animal disease organisms by terrorists; (5) implement a fully secure surveillance and response system that utilizes, or is capable of utilizing, field test devices capable of detecting biological threats to animals and plants and that electronically integrates the devices and the tests on a real-time basis into a comprehensive surveillance, incident management, and emergency response system; (6) implement a plan for coordinating the surveillance for zoonotic disease and human disease (ANSER, S.1715, 2002).

D. LEGISLATION BALANCING PROGRESS VS CONSTRICTION

Having legislation that supports the use of technology in fighting terrorism and crime is a necessary foundation to the long-term effort of keeping the world safe for future generations. But laws are subject to interpretation when delicate circumstances present themselves. Sometimes a court's analysis of the Constitution and a technicality, for example, can render electronic surveillance seemingly useless for enforcing an apparently open and shut indictment—take the following case for example: In June 2001, a U.S. Supreme Court decision determined that in the absence of a search warrant, the government's use of a thermal imaging device to monitor heat coming off the walls of a suspected marijuana grower's private residence in Florence, Oregon, violated the Fourth Amendment prohibition against "unreasonable searches and seizures" (Amato, p. 63). The ruling could have far-reaching consequences for how new, more powerful surveillance technologies can be deployed, managed, and regulated, and how the sensitive databases are protected (Amato, p. 63). As eluded previously, electronic

surveillance is a powerful technology with great law enforcement benefits, but it can backfire if not supported by carefully crafted protocol and legislation (Amato, p. 63).

Several efforts are now under way to rein in surveillance technology through more responsible privacy legislation. The Privacy Coalition, a nonpartisan collection of consumer, labor, and civil liberties groups, is trying to get lawmakers to commit to their "Privacy Pledge," which contains a vow to develop independent oversight of public surveillance technology and limit the collection of personal data. Several organizations, including the AFL-CIO, Communications Workers of America, 9to5, National Association of Working Women, and the United Auto Workers are supporting legislation to restrict electronic monitoring of employees (Amato, p. 63).

In 2000, Congress unsuccessfully debated the Notice of Electronic Monitoring Act (H.R.4908), which would have required companies to notify employees if they were being watched - the bill died in committee. Currently, Connecticut is the only state to require employers to tell employees if they are being monitored (Amato, p. 63).

The very notion of privacy in public is sometimes at odds with certain realities. For example, when individuals go out in public, they look at other people, who in turn look at them, and everyone can see everything around them in visual range—normally people do not try and cover their faces in public to avoid being recognized. So it is a small stretch to imagine a camera looking at people in public—and much like a living police officer, the camera can be programmed to alert for certain unusual sightings or events. Suddenly, our expectation of privacy changes because we are talking about a camera and not merely another living human being looking at us. The logic behind the phobia of surveillance cameras begins to melt away when you think about how boring most of our lives really are in public. We walk, we shop, we commute, we work, we eat, we play in the world we live in—and how often do you see someone attempting to hide their face? The truth reveals itself in the fact that we do not have an expectation of privacy when in public, so if there is a camera in the bank, or store, or parking lot, we generally don't even notice, or mind. Surveillance is becoming ubiquitous because we demand to be safe and orderly as a society. The more violence we see, the more we want law enforcing eyes on scene to come to the rescue when needed, or to present the

recorded surveillance proof in a court of law if necessary. The deployment of surveillance networks may slow down due to public opinion, but it is almost a certainty as we see the samples of its use around the world.

Science fiction author and technology watcher, David Brin, writes in his 1998 book "The Transparent Society" about society facing two versions of ubiquitous surveillance: one in which only the affluent and authoritative use and control the system to their own advantage; the second which depicts a more equitable future where even the watchers can also be watched (Amato, p. 63). The second form of ubiquitous surveillance appears more equitable. In the ubiquitous world, one can imagine an audit trail of every misdeed that can be held to the light of day. For instance - rent a porn video and your wife knows it; but if she drives to your best buddy's house four times a week while you're at the office, you'll know that also (Amato, p. 63). The emerging world of ubiquitous surveillance will grow at a pace set by social and cultural comfort levels. Surveillance and biometric technology seems to be leaping ahead of our ability to govern its service unobtrusively in a society. The will of the people will drive the policies, laws, and guidelines for this technology. The issue of privacy as a commodity is being discussed in government today—should privacy be traded for safety and security in an ever increasingly hostile world? The authors believe it is inevitable but very livable.

E. EXAMPLES OF SURVEILLANCE IMPACT ON SOCIETY

We have seen a glimpse of what ubiquitous surveillance offers, and the debate continues over how best to employ it, but here are some examples hard to refute: Take the case of the "computer-aided drowning detection and prevention" system that Boulogne, France-based Poseidon Technologies has installed in nine swimming pools in France, England, the Netherlands, and Canada (Amato, p. 62). Overhead and in-pool cameras continuously monitors pool activity while feeding the signal to a central processor driven by "perception algorithm" software that can effectively spot when swimmers become still for more than a few seconds. When an abnormal alert is detected, a red alarm light flashes at a poolside laptop workstation, alerting lifeguards via waterproof pagers (Amato, p. 62). In November 2000, a Poseidon system at the Jean Blanchet Aquatic Center in Ancenis, Loire-Atlantique, France, alerted lifeguards in time

to rescue a swimmer on the verge of drowning (Amato, p. 62). Surveillance devices for public safety are now growing rapidly in France; the country now even has public CCTV web cams in nuclear plants to reassure citizens that the work going on is safe and above board (Wakefield, 7 Feb 2002).

The benefits of a sensor rich environment are just beginning. Think of the cascade of mobile gadgets (cell phones, PDAs, watches, automotive navigation systems, etc.) which are being manufactured with Global Positioning System (GPS) transponders built-in, making it possible to pinpoint the signal carrier and rapidly responding to the aid of the individual (Amato, p. 62). In the case of the automobile, an airbag could be designed to give off a transponder signal when it inflates during an accident and automatically call for assistance. The safety benefits of consumer and public ubiquitous surveillance systems are very diverse, and have great potential for cost savings in human resource constrained organizations.

In terms of crime deterrence power, the United Kingdom is still our best metric for analysis. Of the world's 25 million CCTV cameras in use today, 2.5 million are currently in use in the UK; even now, analysts are predicting a tenfold increase in CCTV in the UK over the next five years (Wakefield, 7 Feb 2002). The average citizen in the UK presently is caught on CCTV cameras 300 times a day (Wakefield, 7 Feb 2002). The impact on crime has been profound. Recent British government reports cite closed circuit TV as a major reason for declining crime rates. After these systems were put in place, the town of Berwick reported that burglaries fell by 69 percent; in Northampton, overall crime decreased by 57 percent; and in Glasgow, Scotland, crime slumped by 68 percent (Amato, p. 62). Northampton additionally installed an Automatic Number Plate Recognition system, which resulted in 264 arrests and the recovery of 31 vehicles (BBC, 21 Aug 2001). When 11 cameras were installed in Darlington County, Durham, a 46 percent drop in crime was reported (BBC, 21 Aug 2001). In Somerset, when six cameras were installed in their town center, car thefts fell by more than 50 percent (BBC, 21 Aug 2001). Public reaction in the UK has been mixed however, but many continue to embrace the technology. When strategically employed, the cameras can deter offenders, reducing crime, and increasing the feeling of safety among citizens while in public (BBC,

21 Aug 2001). "I am prepared to exchange a small/negligible amount of privacy loss so I don't have to be caught up in yet another bomb blast/bomb scare," wrote one London resident (Amato, p. 62). According to the UK's Government Crime Reduction Office, law enforcement authorities are convinced of the benefits that CCTV has in reducing crime (Wakefield, 7 Feb 2002). And it's not just the crime prevention aspect CCTV that has the UK singing praise for surveillance, it also saves money by providing an increased number of guilty verdicts in courts through displaying irrefutable proof of the crime (Wakefield, 7 Feb 2002).

Washington DC itself is now undergoing a dramatic surveillance transformation. The National Park Service will begin round-the-clock video surveillance at all major monuments on the district's Mall area by October 2002. The step up in surveillance technology is being met with challenge and protest from the American Civil Liberties Union (ACLU) groups who express concern that video monitoring might discourage lawful and peaceful demonstration on the Mall (Hsu, 22 Mar 2002). Congressional concerns also have been voiced on the oversight, management, and standards for the ubiquitous surveillance initiatives in and around Washington.

Conversely, surveillance and biometric technology in society could be misused if not carefully managed. In the future, motor vehicles agencies will keep a database of drivers with their digital photographs (faceprints) in computer systems that can be networked into a nationwide database capable of tracking an individual's movement in any geographic area. If not protected, this database can be used for unauthorized demographic profiling and spamming in the same way that Internet cookies are used to build demographic profiles to target consumers. On the upside, such a database could be used to enable facial recognition technology to quickly register and verify legitimacy of eligible voters, thus eliminating voter fraud. The illusive issue is that of function creep (a.k.a., mission creep) —allowing a system to be misdirected for another purpose other than its original intent (Amato, p. 63). Tight management of surveillance technology and good procedures can eliminate function creep and keep the system focused toward its intended beneficiaries.

When society thinks of the surveillance debate, the good points at times become overshadowed by Orwellian paranoia. The privacy concerns are warranted, but they need to be weighed unemotionally against the overall benefit to the public, as well as with a sober evaluation of the way we would like to live in this dangerous new world.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION AND RECOMMENDATIONS

A. INTRODUCTION

This thesis has represented a conglomeration of issues surrounding the evolving efforts on the path to homeland security and the potential uses of various surveillance and biometric technologies. In the post-analysis, the research reveals that technology's surveillance response to the war on terrorism is a natural and predictable evolution for managing a world in conflict. We live in a world where sensor-rich environments are becoming commonplace, so it is not a great leap of the imagination to read about surveillance and biometrics leading the way in the war on terrorism and criminal activity. The trend for society to move to these specialized technologies in order to seek improved safety and protection is a controversial but necessary balance of privacy, resource investment, and process efficiency. Technology is merely one part of the total overarching strategy for homeland security; the non-technical human factors and policy assessments must also be carefully considered as we trod down the road of a surveillance society.

While we acknowledge that terrorism and criminal activity cannot be eliminated, technology can certainly aid in detecting, deterring, and markedly reducing the risk. The newly organized Department of Homeland Security, with its supporting legislation and resources, will contribute to the emerging concepts for intelligent employment of surveillance and biometrics. The challenges faced in implementing a balanced strategy for using these technologies seem almost endless, but they can be summarized generally into the following critical success factors that form a basis for the ubiquitous surveillance concept model and recommendations list for further study.

B. CONCLUSIONS, CRITICAL SUCCESS FACTORS, AND RECOMMENDATIONS

1. Human Factors and Incentives for Cultural Change

a. Information Sharing

One of the more evident observations and critical success factors in the quest to enable any system is the ability for people to share information and work

together toward a common goal. Sharing information and vision is crucial in our fight against terrorism. This is the core to managing change in complex organizations. Changing the way governments work at all levels will be a monumental task. Whether it is due to interagency rivalry or separation mandated by administrative protocols, old ways of doing business must be completely reevaluated and realigned toward the new strategic vision. Procedural and psychological barriers to information sharing must not only be dismantled, but incentives need to be established for institutional reorganization that embraces exchange of information and collaboration as the normal order of doing business, not the exception. Performance metrics for personnel and their departments need to be aligned with positive incentives for collaboration. Federal, state, local government, and private sector agencies must work together to encourage alliances for information gathering and closing the intelligence gaps that have allowed previous terrorist and criminal plots to go undetected. Creative solutions for changing cultural paradigms must be developed and implemented to enable information sharing domestically and internationally. Most importantly, the very people who will be affected by these changes in protocol must also be the ones who participate in crafting the necessary new processes and subsequent implementation plans.

b. Supporting Legislation, Standards and Enforcement

The incentive to enact legislation ahead of technology implementation reflects society's desire for maintaining order and fairness. Agencies that become empowered by surveillance and biometrics technology must have the full backing of legislation to be effective. Recent legislation such as the USA Patriot Act, Aviation and Transportation Security Act, Port and Maritime Security Act, and the Bioterrorism Preparedness Act represent only some of the many "change management" initiatives required for establishing policy and direction in addressing technology's role in the war on terror. Numerous other policies are emerging in the form of directives, executive orders, and international treaties. More detailed direction should be tailored in the form of standards and operating procedures for how specific surveillance and biometric applications should be employed and managed throughout all levels of government.

These technologies justifiably capture the attention of civil liberties and privacy groups. Placement of legal controls, guidance, and limitations on how surveillance and biometrics information will be implemented is paramount in safeguarding against potential abuses and unnecessary invasion of privacy. Enforcement of these new laws and standards is as important in safeguarding the rights of law-abiding citizens as they are in detecting and capturing those who wish us harm. Furthermore, enforcement of existing laws must be maximized with respect to our mission. These issues primarily involve procedural policies and principles for society, yet they provide a significant baseline upon which subsequent technical solutions are built and supported.

c. Addressing the Root Causes of Terrorism

Addressing the fundamental catalysts that allow terrorism to flourish is often overlooked. In this light, prevention has its greatest role. Often our technological efforts are reactive to our present day situations and we fail to see the value in heading off the very symptoms that contribute to terrorism and criminal behavior in the first place. Along with recognizing terrorists when they cross our borders, our surveillance efforts must simultaneously focus on the larger global issues that produce regional conflict and world instability: poverty, disease, dwindling natural resources, drug trafficking, religious fanaticism, and proliferation of weapons of mass destruction. Predictive analysis calls for combining data points, drawing inferences on pieces of seemingly disparate information, and establishing early warning indicators that can provide opportunity to fend off disasters in the making. This is where the technical lines of surveillance and biometrics blur with non-technical human factors that beg the question— "if technology cannot rid the world of terrorism, can we at least leverage technology to recognize and preempt conditions and events that contribute to terrorist or criminal activity?" When considering this expanded analysis of the war on terrorism, one begins to see that the real battle is not fought in isolation within the walls of clearly defined boundaries of good versus evil but within the greater "system's view" of a world condition, a "conflict state," which must be contained, monitored and managed. Hence, exploiting the role of surveillance and biometric technology for counter-terrorism is key to prevention. For that reason, the concurrent and inescapable responsibility of

international diplomacy and cooperation in addressing underlying human factors is also an integral critical success factor that technology alone cannot win.

d. The Will of the People and Implementation

The specific question of how to implement a surveillance and biometrics-based system upon an American culture so accustomed to personal freedoms is a difficult one to answer; yet, it is a pivotal critical success factor for the technology. We are already under surveillance when in public—at banks, in department stores, on our roadways, and while in the workplace. Thus, the war on terrorism and America's homeland security initiatives have only expedited an inevitable surveillance society that had been predicted decades earlier by Orwellian prophecy. The technology is ready, but is America and the international community ready? The success factor here may ultimately be measured by the will of the people and the level to which peace-loving nations see value in subjecting their citizens to surveillance. Terrorism is an international problem, and the efforts in arresting it must be global; consequently, international cooperation in implementing the concept of a ubiquitous surveillance grid is paramount. Countries must see the benefit in intelligent uses of surveillance and biometric technology; equally, they must understand that such technologies are capable of preserving the rights of law-abiding citizens. While the greatest motivation for societies to establish a ubiquitous surveillance network may be the prevention of another 9-11, in the end, the financial and economic enticements may ultimately provide the most under-appreciated incentives. It is difficult to argue against creating a more fraud-resistant drivers license, a passport which uses secure biometric technology, or a passenger screening system which quickly and efficiently allows for the processing of millions of passengers a day—saving both time and money. Surveillance and biometrics technologies offer great potential for process efficiencies in managing everything from critical infrastructure protection, to transportation networks, border control, licensing and entitlement controls, and fraud reduction. The intelligence gathering value of this technology is extraordinary; however, implementation must be thoughtful, measured, and balanced to our objectives.

The fear of cultural change alone is a great psychological hurdle on the implementation path for intelligent use of surveillance and biometric technology, yet it is an artificial obstruction that can be overcome with the introduction of proper incentives. As a direct result of 9-11, the will of the majority has spoken and supported strategic implementation of surveillance and biometrics. Americans are now seeing changes taking place as this technology slowly finds its way to improve identification card authentication, workplace access control, transportation hub passenger and cargo screening, monitoring of public places, and a myriad of other useful applications.

Governmental reorganization has already begun, and the formation of the Department of Homeland Security is a necessary beginning in the cultural reshaping, which will pave the way toward the more technical issues of system integration and implementation. The evolving implementation plan for surveillance and biometrics is ongoing and complex. It is worth noting that success in this arena also depends on acquiring the right people with sufficient technical and managerial skills to integrate everything from customs and immigration systems, to our most sophisticated intelligence gathering networks.

2. Establishment of an Enterprise Architecture

The dozens of agencies that make up America's national security and intelligence gathering capability presently utilize an infrastructure, which is not optimized for surveillance information sharing. They function under a variety of different operating system platforms and disparate databases that do not link to one another.

The establishment of common, enterprise-level architecture is necessary and fundamental to support future surveillance integration and information sharing. This enterprise concept would be the foundation of a ubiquitous surveillance network that allows agencies such as the Coast Guard, DoD, U.S. Customs, INS, Border Patrol, TSA, FBI, CIA, NSA, DOJ, FEMA, CDC, HHS, state DMVs, local law enforcement, and emergency responders to share collected information and data mine across a distributed network. Enterprise architecture would also support local, regional, and national healthcare authorities for quickly sharing medical surveillance information and identify emerging biological or chemical threats early, providing faster response to population

centers. The enterprise network would also include linkage to systems that monitor non-human traffic such as postal traffic, cargo container shipments, and other commerce hubs for material goods. The interoperability benefits of a single architecture are vast. Stovepipe and duplicate systems would be eliminated; the synergy of using a common network with collaborative tools would result in efficiencies of speed as well as cost savings. Like a public utility grid, a properly designed surveillance network can be a resource on tap for its users. It would allow connectivity to other existing intelligence information, creating a virtual knowledge portal for information sharing. Even so, any proposed architecture for an enterprise ubiquitous surveillance system should be seen as a supplement to, not replacement for, good human factors in intelligence gathering and predictive analysis. Humans are still the most valuable asset to any systems architecture.

3. Establishment of Surveillance and Biometric Application Standards

This critical success factor speaks to the application and database layers of surveillance and biometrics technology. For this technology to be successfully integrated into an enterprise model, standards must be established for biometric authentication and data capture techniques. If we expect to maintain integrity and interoperability in information, we must begin with providing clear and sanctioned formats for biometric devices and methods of encoding and decoding information. These standards must also address physical and logical security concerns, digital encryption, and network design so the collected information is not intercepted, spoofed, or otherwise abused. Databases and data dictionaries must also have standards for information naming conventions, formats, data types, and data field descriptions so information in one database can easily be related to another without the delay of complex translations. The American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST) should work closely with each other as well as international standards agencies and technical committees for establishing and adopting data standards for an efficient and secure surveillance network.

4. Operational Testing Beyond the Controlled Laboratory Environment

Surveillance and biometric technologies are not perfect or foolproof, although they are steadily improving in accuracy and reliability. Rigorous testing and careful match selection of technology-to-application is extremely important. Chief Information

Officers (CIO) and program managers must be wary of vendors pushing technologies that claim to be ready for real-world homeland security usage. Surveillance and biometric technology programs should not fall victim to the false comfort provided by the successes of earlier, lab-controlled environments. A lab setting may not consider some of the nuances that can greatly influence the performance of the technology in field conditions. Training, operator fatigue, boredom, lighting, temperature, distance, and other factors that cannot always be precisely replicated in a lab may adversely affect the performance of surveillance and biometric systems in real world situations.

Project management milestones must include extensive operational field tests to exercise the technology in the environment for which it is designed. In the case of a State DMV, for example, the agency may utilize biometrics along with proven smart card technology to replace newly issued driver's licenses. User feedback should be carefully examined during these proof-of-concept trials. Such tests would provide valuable lessons-learned; small successes could then be capitalized and improved upon, and unforeseen problems resolved before being mirrored for nationwide or international implementation.

5. Requirements Analysis

The effectiveness of a surveillance and biometrics system is greatly enhanced by conducting thorough efforts in requirements analysis. This can be a very complex and lengthy process but if done properly should result in an effective technology-to-application match with a smooth implementation that is on budget and on schedule. In contrast, a poor job in requirements analysis can lead to a problem-filled project that is over budget, behind schedule, and falls short in meeting the needs of its intended users.

The homeland security strategy touches all areas of human and infrastructure protection activity. Thus, defining the numerous requirements and priorities to be addressed will be crucial for the project managers. This critical success factor is a special challenge since both the technology and requirements seem to be changing simultaneously. It is truly a moving target. Information technology managers must start with taking the idea of a ubiquitous surveillance system, which assumes a "system of systems," and break it down into its more manageable and modularized components.

These components should include requirements for biometric identifiers in human authentication and sensors for chemical, biologic, or other agents. Furthermore, it should address information databases, rules-based identifiers that alert or query action if one or more conditions exist, and linkage for information sharing with and among other systems. The analysis must consider training, ergonomics, and the procedural and process requirements of the system under study. These subcomponents, if in compliance with standards and a common enterprise infrastructure, should be able to interface and exchange information in a larger surveillance grid as more entities are added to the network.

The requirements analysis should also include vulnerabilities and risk assessments as well as functional analysis that reveal how an existing process currently operates. The analysis should reveal information gaps as well as wasteful duplications in the system. In addition, it should examine how the process could either be simplified or otherwise improved upon to address the security requirements, authentication requirements, or surveillance needs of the area in question. However, layering technology and procedures does come at a price in terms of time, money, and convenience; so the process owners must determine a middle ground. The security layering for satisfying these requirements may vary depending on whether one is talking about something as mild as security for public access to a community library or as sensitive as employee access control to a nuclear power plant. The capabilities of various surveillance and biometrics technologies allow us to examine these potential applications with respect to requirements, cost, and efficiency and tailor the design to the security strategy we seek to fill.

The requirements analysis must also examine which entities are responsible for collecting specific information and how this information should be organized, stored, archived, and shared. The sources and methods for enrollment must also be addressed since the basis for biometric systems is to eventually compare profiles against collected information and make decisions based on events or condition states. The ultimate goal is to have an integrated and highly organized "system of systems" by which hybrid links are able to quickly and securely share information about people, places, and things and draw inferences to detect or deter terrorist or criminal threats.

C. CONCEPT MODEL FOR UBIQUITOUS SURVEILLANCE AND BIOMETRICS GRID

The concept for a ubiquitous surveillance and biometrics grid is intended to be broad and non-technical; however, it advocates a plausible overview representation of how this resource might be modeled in the system's view. The previously mentioned critical success factors should be seen as a supplement to this model. The specific examples of where and how surveillance and biometrics might be employed are too numerous to list completely, but we have suggested a handful of probable methods by which key sectors of society may leverage such technology for the future. Figures 7.1 and 7.2 provide a pyramid overview of the surveillance state and conflict state paradigm that we depict and strive to balance and manage.

Figure 7.1. Ubiquitous Surveillance State Concept Pyramid.

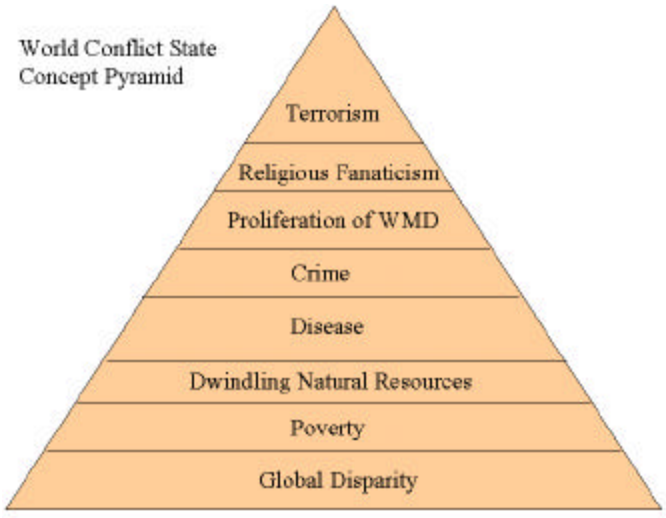


Figure 7.2. World Conflict State Concept Pyramid.

1. Sensor-Rich Environments

For a ubiquitous surveillance system to exist, sensors must be put in place at strategic locations to gather information for initial enrollment, capture, monitoring, and comparative analysis purposes. The type of sensors, their accuracy, capabilities, and locations are important factors in meeting the layered security objectives for what we are trying to protect or monitor.

In the ubiquitous surveillance concept, sensors for biometrics would allow the creation of passports, driver's licenses, visas, and other documents that could then be used to verify that the persons presenting are in fact biologically the individuals they claim to be. A multitude of strategically placed surveillance capabilities would monitor, match, analyze, alert, and suggest varied courses of actions, interventions, and responses. The specialized sensors themselves would perform as a subset in the greater surveillance environment that we already acknowledge as existing in a conflict state—the goal being, to leverage surveillance and biometrics to balance between these two states (see Figure 7.3).

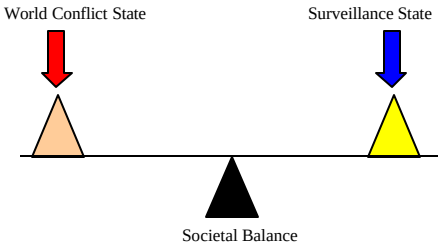


Figure 7.3. Societal Balance.

The following sector areas discuss scenarios for how these technologies could be used in our ubiquitous surveillance model:

a. Aviation

Passenger processing points in transportation hubs would have a combination of sensors that layer non-invasive facial-recognition capabilities with more invasive sensors such as fingerprint, hand and iris scanners, which authenticate passenger identities at embarkation. These sensors would be connected to an enterprise infrastructure that checks passenger identities against distributed databases of wanted lists and alert conditions. Full-body scanners would be able to detect any weapons or unauthorized items a person may be wearing. Within the aircraft, discrete video cameras in the cabin would allow the aircrew to monitor passenger activity, permitting early warning, as well as documenting evidence of threatening behavior such as air rage or other actions that would jeopardize flight safety. Trained plain-clothed air marshals would supplement the technology by monitoring for suspicious activity requiring attention. Sensors capable of spotting weapons and trace amounts of chemical, biological, and other hazardous materials would scan baggage and air cargo. Surveillance cameras and environmental sensors in and around the airport facility would monitor for any suspicious activity.

b. Seaport/Maritime

Sensors installed at seaports would include scanners for visual examination of cargo container contents. International cooperation would establish

standardized scanning procedures and capabilities at all cargo embarkation points. Specialized sensors would also be installed to detect any chemical, biological, or nuclear materials present at embarkation and debarkation points. The use of trained dogs and human inspectors would supplement surveillance of cargo for contents that may elude sensors, such as illegal drugs, explosives, or human cargo. Surface and undersea sensors at harbors and piers would detect for any suspicious water activity such as unauthorized scuba divers or undersea craft.

c. Customs and Border Control

Sensors installed at borders would include similar capabilities set forth in the aviation and seaport sectors. Additionally, biometric scanners would automatically enroll visitors, compare individuals against a database of wanted lists, and validate the identities of individuals with existing biometric identification cards. These smart borders would also include infrared, motion, night-vision sensors, and surveillance cameras that would monitor areas that are particularly vulnerable, alerting authorities to a compromise.

d. Sensitive Access to Critical Work Environment

Sensors installed at access points in the workplace would aid in keeping unauthorized personnel out of sensitive areas while allowing authorized employees privilege-based entry to specified areas within facility walls. Biometric supported secure smart cards would be the norm for access to all areas considered critical to national infrastructure. Digital video surveillance in parking lots, entryways, and loading zones would capture traffic activity and allow intelligent software algorithms to alert authorities to any suspicious patterns or possible threat conditions. This secure access would provide flexible levels of protection for environments where critical infrastructure is housed, such as energy, telecommunications, defense, healthcare, financial sectors, and transportation hubs. These sensors would serve as authentication tools as well as audit trails for an individual's movement through the physical environment as well as cyber environment. Intelligent software agents would also monitor workplace system network traffic and Internet packets looking for conditions that may indicate unauthorized access or behaviors requiring further investigation.

A nationally approved biometrics-based identification card would serve as a replacement for the social security card and thereby establish a common proof of individual authentication and entitlements validation for citizens. Digitally encrypted biometrics in combination with secure PINs would ensure that the combination of "who you are biologically" and "what you know" (PIN) produce a tamper-resistant authentication card.

e. Environmental, Agricultural, and Public Grounds Surveillance

Sensors installed at strategic locations in the environment and agricultural centers would collect and analyze information from the air, water, and soil in order to monitor for chemical, biological, nuclear, or other agents that may require action by authorities. Farm produce, animal, and food processing centers would likewise be configured with sensors that monitor for hazardous agents and alert to preset conditions.

Strategically placed detection devices and video surveillance at public grounds would further ensure environments around our roadways, bridges, tunnels, recreation areas, school grounds, and key population centers are safe. These video surveillance cameras would not only serve to alert to terrorist or criminal activity, but they would also provide for rapid response for other emergency situations such as vehicle accidents, pollution spills, forest fires, or any number of calamities.

f. Medical Surveillance

Effective medical surveillance components would be comprised of intelligent medical networks that alert authorities to any signs of epidemiological and infectious disease outbreaks. These networks would be capable of determining if the disease surveillance indicators are out of normal ranges for a particular area or season and would furthermore enable modeling and simulation to forecast possible spread patterns and containment strategies. Local and regional medical centers would be linked with medical suppliers, pharmaceutical companies, and drug store databases to alert to any unusual orders for supplies or prescription and non-prescription drugs that may correlate with disease outbreaks. All medical centers would be linked with Centers for Disease Control (CDC), Health and Human Services (HHS), National Institute of Health (NIH), and the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) to

collaborate, respond to, and counter any possible national health crisis. The United States Department of Agriculture (USDA), Animal and Plant Health Inspection Service (APHIS) and U.S. Customs Service would also be integrated to the medical surveillance network to share any contributing animal, plant, or food related surveillance information that may affect disease control and management. Furthermore, national medical networks would be connected with the World Health Organization (WHO) and International Red Cross to collaborate in response and management of disease outbreaks as well as subsequent humanitarian efforts.

g. Space-Based and Airborne Surveillance Vehicles

Sensors in spaced-based satellites and Unmanned Aerial Vehicles (UAV) would allow for surveillance of environmental conditions or other anomalies that warrant our attention. Surveillance from space allows us to monitor changes in everything from meteorological and geographical conditions to movements of military weapons and personnel. Advancements in thermal and hyperspectral imaging enable us to detect changes previously hidden to the naked eye. UAVs would also be equipped with remote sensing devices to sniff for chemical, biological, or other hazardous agents, giving early warning of any dangers. Surveillance use of Unmanned Combat Aerial Vehicles (UCAV) would also allow us to response with force to a threat condition in near real-time if required.

2. Information Portals, Knowledge Bases and Collaborative Environments

Albert Einstein once said "Not everything that counts can be counted, and not everything that can be counted counts." As we drown in a sea of potentially useful information, we seek only that which is truly relevant to our task. Information portals and knowledge management are established concepts of information access and data management; hence, the notion of a single starting point for information searches and assembling mazes of data into meaningful resources is not new to Internet savvy users. Internet portals have been with us for years, and the time has come that an equivalent design be considered for Homeland Security information sharing. By virtue of their function, ubiquitous surveillance and biometric technologies, collect, store, and compare information. The off-the-shelf technologies that allow data warehousing, information

access, analysis, and knowledge management must be used to integrate and manage the volumes of data, which will populate the ubiquitous surveillance grid of the future. Through a common portal that is linked to a network of distributed data warehouses and decision support and analytical engines, agencies can more efficiently locate and analyze bits of information to see a larger picture of human behavior, materials movement, and threat conditions, which may warrant our intervention. Sophisticated modeling and simulation programs using knowledge bases of surveillance and biometric information would allow us to perform predictive analysis to better mitigate our vulnerabilities and strengthen our procedures where necessary. Secure collaborative cyber environments would allow emergency responders, intelligence, and law enforcement authorities to work together across distances and exchange vital information.

3. Global Standards

The ubiquitous surveillance model relies heavily on standards for sharing and transporting large volumes of stored information in distributed databases. These standards must not only address naming conventions, data compatibility issues, algorithms, protocols, and operating procedures, but also the transnational security issues of data privacy for surveillance and biometric information. Standardized biometric identifiers could be digitally encrypted to provide security of the embedded information. Pier-to-pier standards could allow for powerful grid computing capabilities that would maximize computing power, eliminate stovepipe systems, and provide efficient access and data-mining across numerous databases. Global standards would enable the synergy for analytical engines to model, simulate, and suggest probable courses of action to counter threat conditions and minimize vulnerabilities.

D. FUTURE RESEARCH

The breadth this thesis research has taken in trying to address the numerous issues of surveillance and biometrics in homeland security has both amazed and engaged the authors. The challenges are complex, and the road ahead will be a long and controversial one for these technologies. Unfortunately, we do not have the luxury of time; we must begin to use our proven technologies now toward the goals of homeland security and diligently work to improve them as we move ever forward. The most important lesson learned from this study is that there is no single solution to winning the war on

terrorism—it will be both a challenge for technology as well as for human cooperation. We have found that although technical solutions exist and hold great promise to assist in the homeland security effort, success will ultimately be a function of complex human factors and unprecedented national and international cooperation. Recommended areas for more in-depth study include but are not limited to the topics listed in Table 7.1.

Recommended Areas for Further Thesis Study	
- aircraft onboard cabin video surveillance - artificial intelligence - cargo screening technologies - chemical, biological, and nuclear detection technologies - collaborative information sharing technologies - computer forensics - computer modeling and simulation - critical infrastructure protection - decision support systems - enterprise architecture - enterprise storage - foreign policy - fuzzy logic - globalization impact on world conflict - grid computing - human factors in IT implementation - impact of technology on privacy	- inference and analytical engines - information warfare - infrastructure protection - international cooperation - knowledge management - managing change in complex organizations - management information bases - medical surveillance technologies - mobile robotic surveillance technology multiagent systems - network security for surveillance - neural networks - predictive analysis - project management - smart card technology - terrorist networks - ubiquitous computing - wireless surveillance and mobile biometric devices

Table 7.1. Recommended Areas for Further Thesis Study.

E. SUMMARY

This chapter provides a depiction for probable implementation areas within a ubiquitous surveillance and biometrics society. The concept does not purport to be the solution for ending terrorism, but it is an enabler amid a collection of resources. Terrorism is but one of many symptoms of a world in conflict; and conflict must be managed. The research has confirmed that although technology will play a pivotal role in homeland security, it is people who are the most important ingredients in leveraging its benefits. People can produce synergy through technology by sharing information, establishing standards and procedures, providing proper training, and exercising good judgment.

Our ability to cooperate domestically and internationally as neighbors of one world will be tested in the months and years ahead, as we implement the initiatives required for making the world a safer place for civilization. The areas this thesis covered during the research period are as broad as they are controversial. Much study still needs to be done on the specific details of how best to plan and implement surveillance and biometrics initiatives. There is great value in learning lessons from other countries that have had successes with respect to their own homeland security related efforts—the United Kingdom and Israel in particular. The potential benefits of this technology surpass counter-terrorism aims; crime reduction, fraud reduction, improved transportation safety, better quality control in commerce, efficient immigration, and border management are just some of the advantages of intelligent surveillance and biometrics employment.

Finally, as we listen to debates on civil liberties and privacy for and against this technology as surveillance incrementally makes its way into our everyday lives, we need to stop and ask ourselves—what price are we willing to pay to feel safe again? It becomes a complex equation for consequence management. One terrorist with one weapon of mass destruction can kill millions. What price would you pay? Society is forming its own answer now and the resulting environment should provide for a more stable and manageable world.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. CHRONOLOGY OF HOMELAND SECURITY, POST 11 SEPTEMBER 2001 (FROM WHITEHOUSE, JUN 2002)

Sep 11, 2001:	America attacked.
Sep 11, 2001:	Department of Defense begins combat air patrols over U.S. cities.
Sep 11, 2001:	Department of Transportation grounds all U.S. private aircraft.
Sep 11, 2001:	FEMA activates Federal Response Plan.
Sep 11, 2001:	U.S. Customs goes to Level 1 alert at all border ports of entry.
Sep 11, 2001:	HHS activates (for the first time ever) the National Disaster Medical System, dispatching more than 300 medical and mortuary personnel to the New York and Washington, D.C. areas, dispatching one of eight 12-hour emergency "push packages" of medical supplies, and putting 80 Disaster Medical Assistance Teams nationwide and 7,000 private sector medical professionals on deployment alert.
Sep 11, 2001:	Nuclear Regulatory Commission advises all nuclear power plants, non-power reactors, nuclear fuel facilities and gaseous diffusion plants go to the highest level of security. All complied.
Sep 11, 2001:	President orders federal disaster funding for New York.
Sep 11, 2001:	FEMA deploys National Urban Search and Rescue Response team.
Sep 11, 2001:	FEMA deploys US Army Corp of Engineers to assist debris removal.
Sep 12, 2001:	FEMA deploys emergency medical and mortuary teams to NY and Washington.
Sep 12, 2001:	FAA allows limited reopening of the nation's commercial airspace system to allow flights that were diverted on September 11 to continue to their original destinations.
Sep 13, 2001:	President orders federal aid for Virginia.
Sep 13, 2001:	Departments of Justice and Treasury deploy Marshals, Border Patrol, and Customs officials to provide a larger police presence at airports as they reopen.
Sep 14, 2001:	President proclaims a national emergency (Proc. 7463).
Sep 14, 2001:	President orders ready reserves of armed forces to active duty.
Sep 14, 2001:	FBI Releases List of Nineteen Suspected Terrorists.
Sep 17, 2001:	Attorney General directs the establishment of 94 Anti-Terrorism Task Forces, one for each United States Attorney Office.

Sep 18, 2001:	President signs authorization for Use of Military Force bill.
Sep 18, 2001:	President authorizes additional disaster funding for New York.
Sep 20, 2001:	President addresses Congress, announces creation of the Office of Homeland Security and appointment of Governor Tom Ridge as Director.
Sep 21, 2001:	HHS announces that more than $126 million (part of $5 billion the President released for disaster relief) is being provided immediately to support health services provided in the wake of the attacks.
Sep 22, 2001:	President signs airline transportation legislation, providing tools to assure the safety and immediate stability of our Nation's commercial airline system, and establish a process for compensating victims of the terrorist attacks.
Sep 25, 2001:	The first of approximately 7,200 National Guard troops begin augmenting security at 444 airports.
Sep 27, 2001:	The FBI releases photographs of 19 individuals believed to be the 9/11 hijackers Sep Coast Guard immediately mobilized more than 2,000 Reservists in the largest homeland defense and port security operation since World War II.
Oct 1, 2001:	FEMA declares over $344 million committed to New York recovery so far.
Oct 4, 2001:	Robert Stevens dies of anthrax in Florida – first known victim of biological terrorism.
Oct 8, 2001:	President swears-in Governor Ridge as Assistant to the President for Homeland Security, and issues Executive Order creating OHS.
Oct 9, 2001:	President swears-in General (Retired) Wayne Downing as Director of the Office of Combating Terrorism, and issues Executive order creating OCT.
Oct 10, 2001:	President unveils "most wanted" terrorists.
Oct 12, 2001:	FAA restores general aviation in 15 major metropolitan areas.
Oct 16, 2001:	President issues Executive Order establishing the President's Critical Infrastructure Protection Board to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems.
Oct 21, 2001:	FAA restores general aviation in 12 more major metropolitan areas.
Oct 22, 2001:	President issues Executive Order for HHS to exercise certain contracting authority in connection with national defense functions.

Oct 23, 2001:	U.S. Customs Service creates new Office of Anti-Terrorism.
Oct 25, 2001:	Department of Treasury launches Operation Greenquest, a new multi-agency financial enforcement initiative bringing the full scope of the government's financial expertise to bear against sources of terrorist funding.
Oct 26, 2001:	President signs the USA Patriot Act.
Oct 29, 2001:	President chairs first meeting of the Homeland Security Council. Issues Homeland Security Presidential Directive-1, establishing the organization and operation of the HSC, and HSPD-2, establishing the Foreign Terrorist Tracking Task Force and increasing immigration vigilance.
Oct 30, 2001:	FAA restricts all private aircraft flying over nuclear facilities.
Nov 8, 2001:	President announces that the Corporation for National and Community Service (CNCS) will support homeland security, mobilizing more than 20,000 Senior Corps and AmeriCorps participants.
Nov 8, 2001:	President Bush creates the Presidential Task Force on Citizen Preparedness in the War Against Terrorism to help prepare Americans in their homes, neighborhoods, schools, workplaces, places of worship, and public places from the potential consequences of terrorist attacks.
Nov 15, 2001:	FEMA announces Individual and Family Grant program for disaster assistance
Nov 28, 2001:	HHS awards contract to produce 155 million doses of smallpox vaccine by the end of 2002 to bring the total of doses in the nation's stockpile to 286 million, enough to protect every United States citizen.
Nov 29, 2001:	Attorney General Ashcroft announces Responsible Cooperators Program, which will provide immigration benefits to non-citizens who furnish information to help apprehend terrorists or to stop terrorist attacks.
Dec 3, 2001:	FBI implements first phase of headquarters reorganization.
Dec 10, 2001:	U.S. Customs launches “Operation Shield America” to prevent international terrorist organizations from obtaining sensitive U.S. technology, weapons, and other equipment.
Dec 12, 2001:	Governor Ridge and Canadian Foreign Minister John Manley sign a “smart border” declaration and action plan to improve security and efficiency of the Northern border.
Dec 19, 2001:	FAA restores general aviation in 30 major metropolitan areas.

Dec 28, 2001:	President issues Executive Orders on succession in federal agencies.
Jan 10, 2002:	President signs $2.9 billion bioterrorism appropriations bill.
Jan 11, 2002:	FAA publishes new standards to protect cockpits fom intrusion and small arms fire or fragmentation devices, such as grenades, requiring operators of more than 6,000 airplanes to install reinforced doors by April 9, 2003.
Jan 17, 2002:	President issues Executive Order authorizing the Secretary of Transportation to increase the number of Coast Guard service members on active duty.
Jan 17, 2002:	U.S. Customs announces Container Security Initiative.
Jan 17-18, 2002:	U.S. Border Patrol officials and other representatives of the INS meet with Native American leaders and law enforcement officials jointly strengthen security along the Southwest and Northern borders.
Jan 17, 2002:	FBI releases information, photographs, and FBI laboratory photographic retouches Jan 25 on six suspected terrorists.
Jan 18, 2002:	Department of Transportation meets mandate to submit plans for training security screeners and flight crews Jan 23 FBI announces new hiring initiative for FBI Special Agents.
Jan 28, 2002:	Congress confirms appointment of John W. Magaw as Under Secretary of Transportation for Security.
Jan 30, 2002:	President issues Executive Order establishing the USA Freedom Corps, encouraging all Americans to serve their country for the equivalent of at least 2 years (4,000 hours) over their lifetimes.
Jan 31, 2002:	HHS announces state allotments of $1.1 billion to help strengthen their capacity to respond to bioterrorism and other public health emergencies resulting from terrorism.
Feb 3, 2002:	United States Secret Service ensures security of Super Bowl XXXVI, a National Special Security Event.
Feb 4, 2002:	President submits the President's Budget for FY 2003 to the Congress, directing $37.7 billion to homeland security, up from $19.5 billion in FY 2002.
Feb 6, 2002:	Attorney General Ashcroft announces rule change to Board of Immigration Appeals to eliminate backlog, prevent unwarranted delays, and improve the quality of board decision-making while ensuring that those in our immigration court system enjoy the full protections of due process.

Feb 8-24, 2002: United States Secret Service ensures security of the 2002 Winter Olympics, a National Special Security Event Feb 25 Soldiers of the U.S. Army National Guard begin to deploy to augment border Security.

Feb 26, 2002: Nuclear Regulatory Commission orders all 104 commercial nuclear power plants to implement interim compensatory security measures, formalizing measures taken in response to NRC advisories since September 11, and imposing additional security enhancements because of on-going comprehensive security review.

Mar 1, 2002: U.S. Customs Service announces action plan to ensure international air carrier compliance with regulations requiring passenger and crew information prior to arrival in the U.S. on flights from foreign locations.

Mar 5, 2002: Attorney General Ashcroft announces National Security Coordination Council to ensure seamless coordination of all functions of the Department of Justice relating to national security, particularly efforts to combat terrorism.

Mar 8, 2002: To date, the U.S. Coast Guard has conducted over 35,000 port security patrols and 3,500 air patrols; boarded over 10,000 vessels including over 2,000 "high interest vessels;" escorted 6,000 vessels in and out of ports including 2,000 escorted by Sea Marshalls; maintained over 124 security zones; and recalled 2,900 Reservists to active duty.

Mar 12, 2002: President establishes the Homeland Security Advisory System (HSPD-3).

Mar 19, 2002: President issues Executive Order establishing the President's Homeland Security Advisory Council.

Mar 22, 2002: Secretary of State Powell and Mexico Interior Minister Santiago Creel sign a "smart border" declaration and action plan to improve security and efficiency of the Southern border.

Mar 25, 2002: U.S. Customs officers begin partnership with Canadian Customs officers to inspect U.S.- bound cargo upon its first arrival in the ports of Montreal, Halifax, and Vancouver.

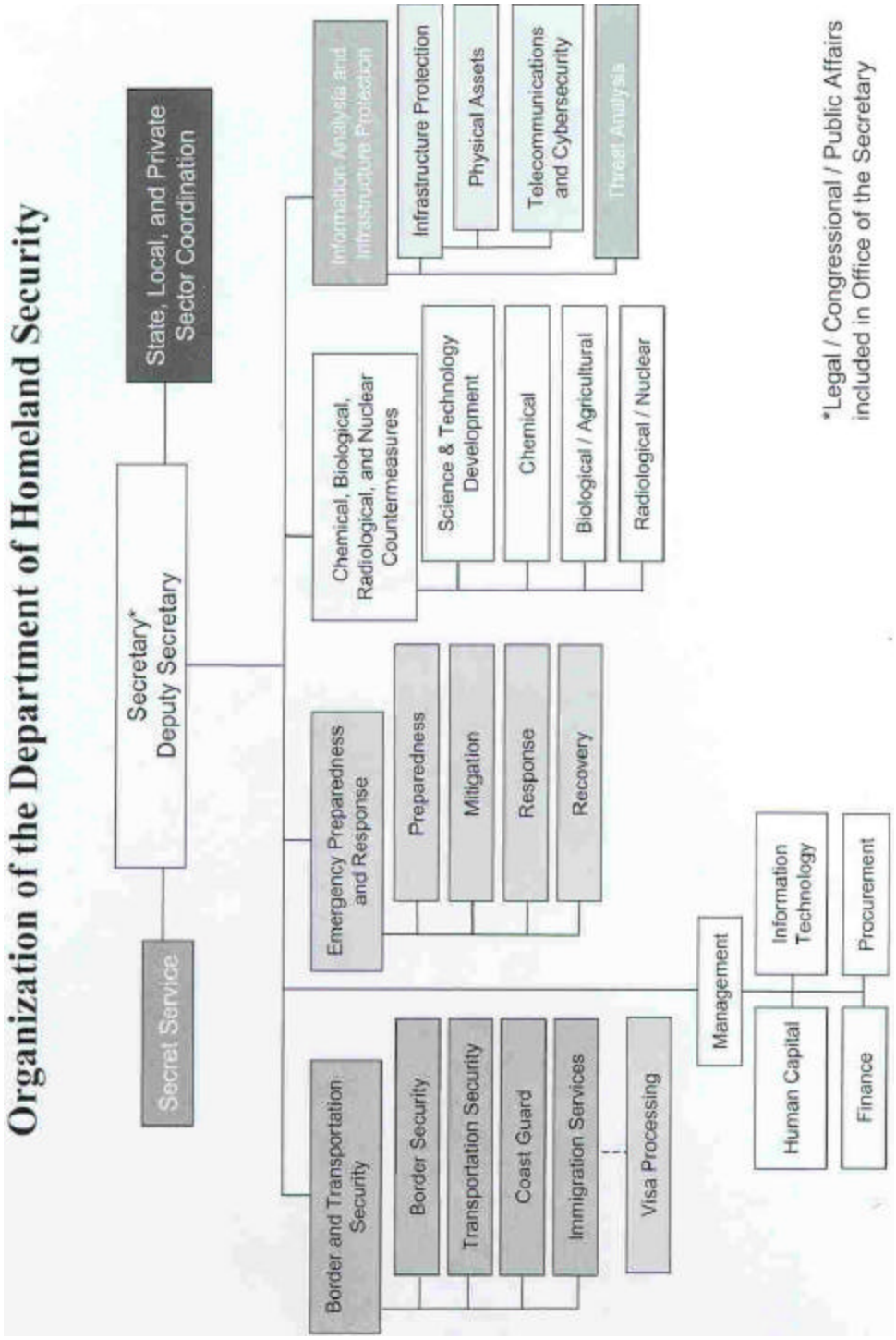
Mar 25, 2002: Nuclear Regulatory Commission orders Honeywell International, Inc., a uranium conversion. facility in Illinois, to implement interim compensatory security measures.

Mar 29, 2002: HHS announces it will obtain more than 75 million additional doses of smallpox vaccine from Aventis Pasteur Inc., provided the supply, stored in a secure location since 1972, and is proven safe and effective Apr 5. NRC forms Office of Security to streamline security, safeguards, and incident response activities.

Apr 8, 2002:	INS implements rule changes governing an alien's ability to begin a course of study the period of time visitors are permitted to remain in the United States.
Apr 16, 2002:	U.S. Customs launches the Customs-Trade Partnership Against Terrorism.
Apr 22, 2002:	FBI Director Mueller announces key management positions in the counterterrorism division.
Apr 30, 2002:	Transportation Security Administration announces successful implementation of Federal passenger screeners at Baltimore-Washington airport.
May 14, 2002:	President Signs Border Security and Visa Entry Reform Act.
May 19, 2002:	TSA issues 180-day progress report to Congress.
May 22, 2002:	CIA creates new position of Associate Director of Central Intelligence for Homeland Security, effective May 28.
May 24, 2002:	Nuclear Regulatory Commission orders decommissioning of commercial nuclear power plants with spent fuel stored in water-filled pools and a spent nuclear fuel storage facility using pool storage to implement interim compensatory security measures for the current threat environment.
May 29, 2002:	Attorney General Ashcroft and FBI Director Mueller announce reorganization of the FBI to achieve top priority of counter-terrorism and better coordination with the CIA.

Source: Whitehouse, June 2002.

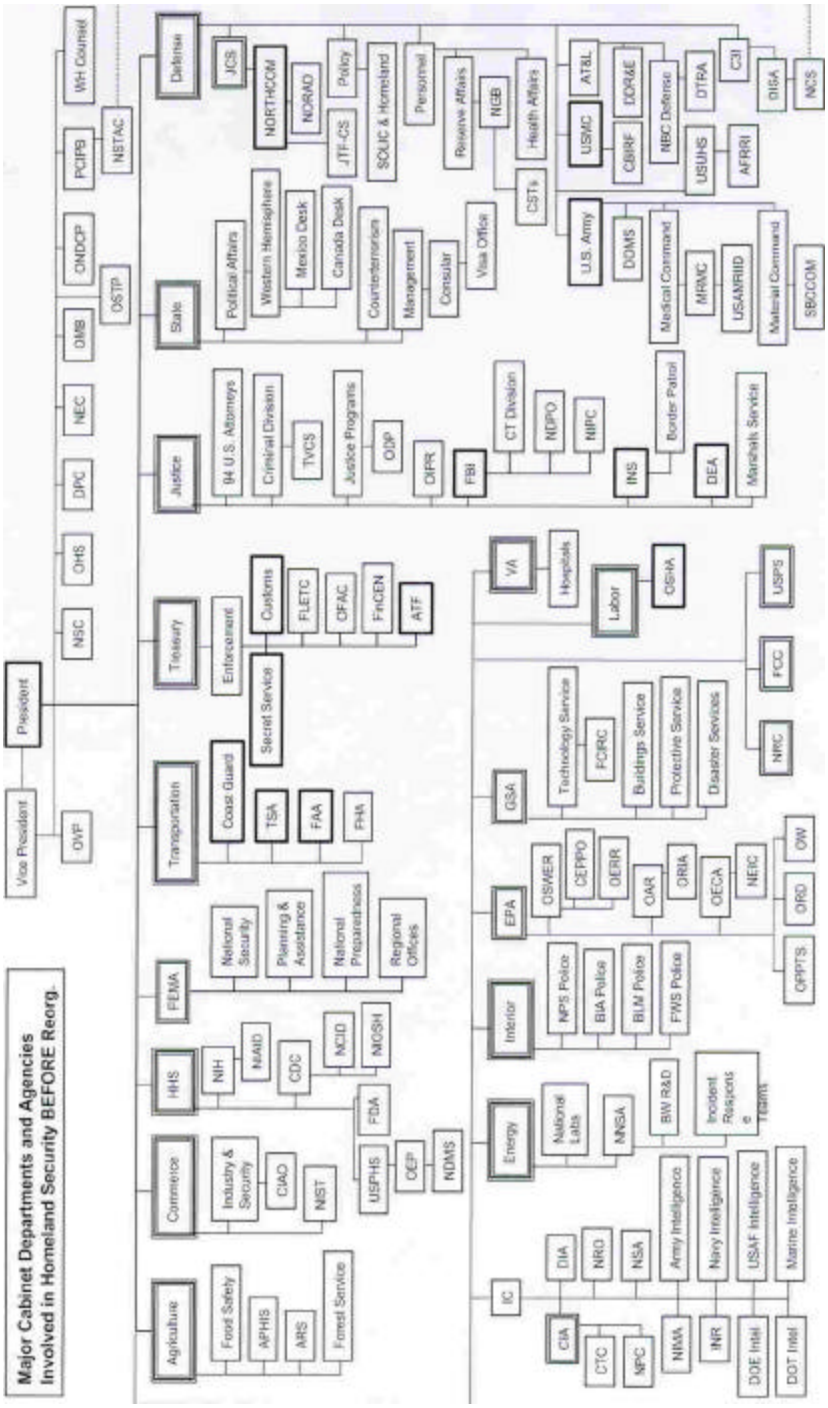
APPENDIX B. ORGANIZATION OF THE HOMELAND SECURITY DEPARTMENT



Source: Whitehouse, June 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

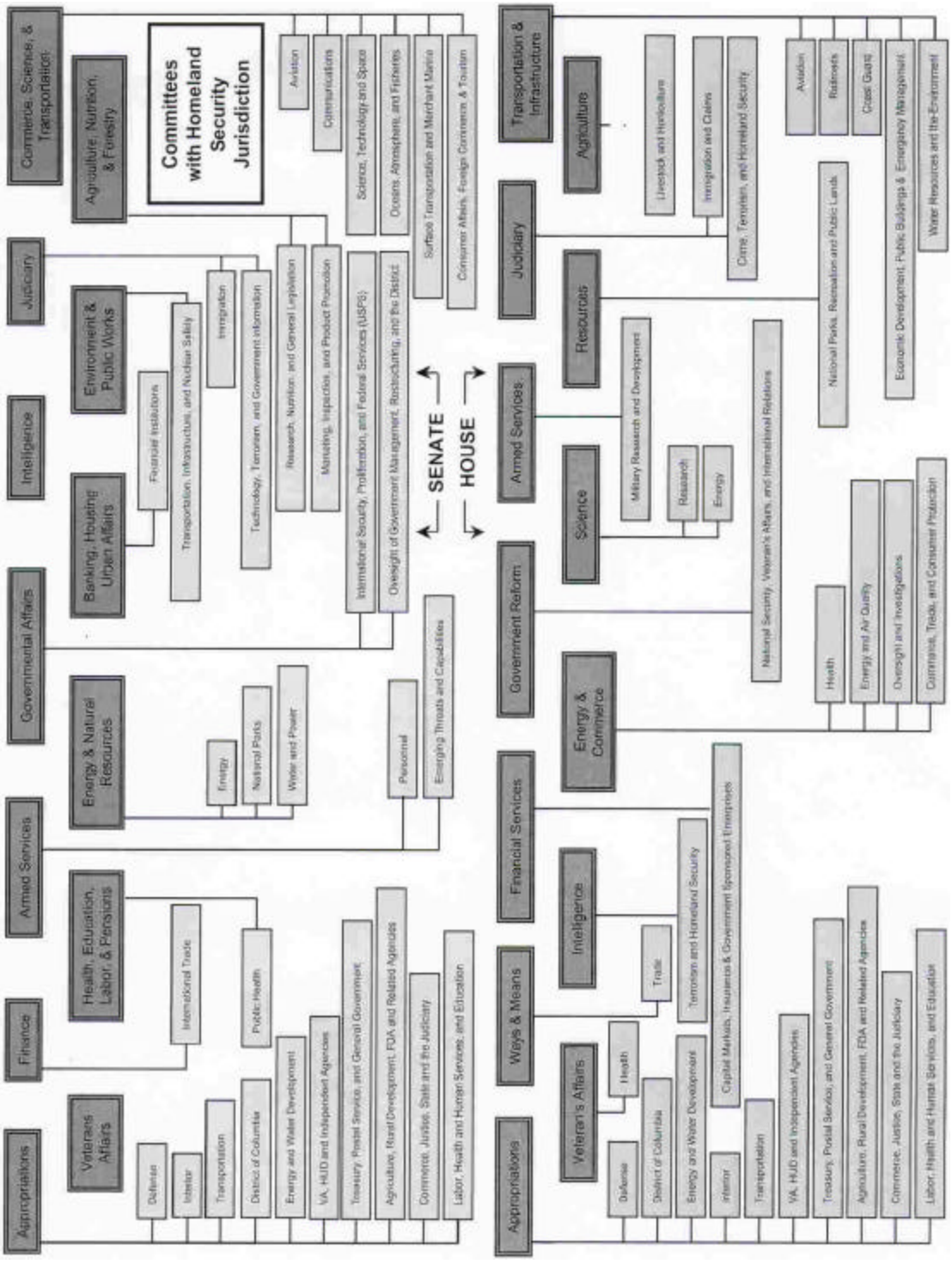
APPENDIX C. MAJOR CABINET AND AGENCIES INVOLVED IN HOMELAND SECURITY BEFORE REORGANIZATION



Source: Whitehouse, June 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. HOMELAND SECURITY JURISDICTION



Source: Whitehouse, June 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. BIOMETRICS GLOSSARY

Algorithm

A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template are a match.

American National Standards Institute (ANSI)

Established in 1918, ANSI is a voluntary organization that creates standards for the computer industry. The FBI commissioned ANSI to create an image standard for the exchange of fingerprint data between AFIS systems.

Application Programming Interface (API)

A set of services or instructions used to standardize an application.

Attempt

The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.

Authentication

The action of verifying information such as identity, ownership, or authorization. The preferred biometric term is verification.

Authentication Routine

A cryptographic process used to validate a user, card, terminal, or message contents. Also known as a handshake, the routine uses important data to create a code that can be verified in real time or batch mode. (see verification)

Automated Fingerprint Identification System (AFIS)

A specialized biometric system that compares a single finger image with a database of finger images. In law enforcement, AFIS is used to collect fingerprints from

criminal suspects and crime scenes. In civilian life, fingerprint scanners are used to identify employees, protect sensitive data, etc.

Automatic ID/Auto ID

An umbrella term for any biometric system or other security technology that uses automatic means to check identity. This applies to both one-to-one verification and one-to-many identification.

Behavioral Biometric

A biometric that is characterized by a behavioral trait that is learned and acquired over time, rather than a physical or physiological characteristic. (contrast with physical biometric)

Bifurcation

A branch made by more than one finger image ridge.

Binning

Taking advantage of different fingerprint pattern classifications to reduce the number of comparisons that must be performed to find a match in an identification system. Enrolled fingerprints that can be classified with a high degree of confidence are assigned to "bins" corresponding to each classification. A submitted print that cannot be classified with high confidence must be matched against all the bins (the entire database), but prints that can be classified need only be matched against the corresponding bin or bins.

Biometric

A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee.

Biometric Application Programming Interface (BAPI)

This is an API that allows the programmer to develop applications for a broad range of virtual biometric devices (VBDs) without knowing the specific capabilities of

the device. The API is comprised of three distinct levels of functionality from high device abstraction to low (device specific) abstraction.

Biometric System

An automated system capable of capturing a biometric sample from an end user; extracting biometric data from that sample; comparing the biometric data with that contained in one or more reference templates; deciding how well they match; and indicating whether or not an identification or verification of identity has been achieved.

Biometrics

The automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic to a comprehensive database for purposes of identification.

Block Cipher

A symmetric cipher, which encrypts a message by breaking it down into blocks and encrypting each block.

BPI

Bits per inch, as on a magnetic stripe card.

CAPI

Cryptographic Application Programming Interface.

CSP

Cryptographic Service Provider.

Capture

The method of taking a biometric sample from the end user.

Cipher

An encryption/decryption algorithm.

Ciphertext

Encrypted data.

Classification

A scheme for categorizing fingerprints according to their overall patterns. Some fingers do not fit into any of the classes, and some may have attributes of more than one class. (see binning)

Coding

Image processing software for extracting minutiae features from the image.

Comparison

The process of comparing a biometric sample with a previously stored reference template or templates. (see one-to-many and one-to-one)

Cryptography

The art and science of using mathematics to secure information and create a high degree of trust in the electronic realm. (see public key and private key)

Cryptographic Key

(see key and public key)

Cryptosystem

An encryption/decryption algorithm (cipher), together with all possible plaintexts, ciphertexts and keys.

Data Encryption Standard (DES)

Data Encryption Standard, a block cipher developed by IBM and the U.S. Government in the 1970s as an official standard.

Decryption

The inverse (reverse) of encryption.

Demographic Data

Census information about an individual, such as name, address, gender, race, and year of birth.

Digital Signature

The encryption of a message digest with a private key.

Direct Fingerprint Reader (DFR)

A device capable of scanning finger images directly from an individual's fingers.

Electronic Benefits Transfer (EBT)

Electronic Benefits Transfer enables automatic benefits distribution. It is currently implemented in WIC and Food Stamps programs.

Encryption

The transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone who has the key that decrypts (undoes the encryption of) the ciphertext.

End User

A person who interacts with a biometric system to enroll or have his/her identity checked.

Enrollee

A person who has a biometric reference template on file.

Enrollment

The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrollment Time

The time a person must spend to have his/her biometric reference template successfully created.

Enrollment Station

A workstation at which an individual's biometrics (fingerprint, voiceprint, etc.) and personal information (name, address, etc.) can be entered into a bioidentification system.

Extraction

The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

False Acceptance Rate (FAR)

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. Also known as the Type II error rate.

False Rejection Rate (FRR)

The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. Also known as the Type I error rate.

Fingerprint Identification Unit (FIU)

A biometric system capable of capturing, storing, and comparing fingerprint data for the purposes of verifying an individual's identity.

Fingerprint Template

A description of all the detected minutiae in a fingerprint pattern. The template contains each minutia's x/y coordinate, slope, and type, thus summarizing the characteristics of the fingerprint for purposes of matching the fingerprint against candidates.

Identification

A one-to-many comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity within a database, rather than verify a claimed identity. (contrast with verification)

Image Database

The database that contains all fingerprint templates in the system. The image database can contain images of the fingerprints, as well as photograph and signature images.

International Standards Organization (ISO)

The major international standards-setting organization for cards of all types.

Key

A string of bits used widely in cryptography, allowing people to encrypt and decrypt data; a key can be used to perform other mathematical operations as well. Given a cipher, a key determines the mapping of the plaintext to the ciphertext. (see private key and public key)

Key Management

The various processes that deal with the creation, distribution, authentication, and storage of keys.

Live Capture

The process of capturing a biometric sample by an interaction between an end user and a biometric system.

Match/Matching

The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

Minutiae

Points corresponding to the ridge endings, deltas, and bifurcations of a finger pattern. Minutiae are described in a fingerprint template.

Minutiae Database

The database that contains all fingerprint templates in the system. The minutiae database is contained within the image database.

Non-repudiation

A property of a cryptosystem. Non-repudiation cryptosystems are those in which the users cannot deny actions they performed.

One-to-Many

Fingerprint search that compares the minutiae from a candidate fingerprint image against the fingerprint minutiae database to determine whether the candidate exists in the database. (synonym for identification.)

One-to-One

Fingerprint search that compares the minutiae from an individual's live fingerprint image against fingerprint minutiae stored on a card or in a specific database record to determine whether or not the individual is who he or she claims to be. (synonym for verification.)

Original Equipment Manufacturer (OEM)

A biometric organization (manufacturer) that assembles a complete biometric system from parts, or assembles a biometric module for integration into a complete biometric system.

Password Bank

A database for storing username, password, and other personal information, to be released upon verification of an individual's identity.

Personal Identification Number (PIN)

A security method whereby a (usually) four-digit number is entered by an individual to gain access to a particular system or area.

Physical/Physiological Biometric

A biometric that is characterized by a physical characteristic rather than a behavioral trait. (contrast with behavioral biometric)

Plaintext

The data to be encrypted.

Private Key

In public-key cryptography, this key is the secret key. It is primarily used for decryption but is also used for encryption with digital signatures.

Public Key

In public-key cryptography, this key is made public to all. It is primarily used for encryption but can be used for verifying signatures.

Public Key Cryptography

Cryptography based on methods involving a public key and a private key.

Public Key Infrastructure (PKI)

PKIs are designed to solve the key management problem. (see key management)

Password List (PWL)

A database for storing username, password, and other personal information, to be released upon verification of an individual's identity.

Recognition

The preferred term is identification.

Reference Template

Data that represents the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Registration

Process of registering biometric data with a Fingerprint Identification Unit (FIU) or other biometric system.

Rejection/False Rejection

When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee. Also known as a Type I error.

Response Time/Processing Time

The time period required by a biometric system to return a decision on identification or verification of a biometric sample.

Smart Card

A card-shaped portable data carrier that contains one or more integrated circuits for data storage and processing. A typical smart card chip includes a microprocessor or CPU, ROM (for storing operating instructions), RAM (for storing data during processing), and EPROM (or EEPROM) memory for nonvolatile storage of information.

Software Developer's Kit (SDK)

A programming package that enables a programmer to develop applications for a specific platform. Typically, an SDK includes one or more APIs, programming tools, and documentation.

Threshold

The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.

Type I Error

The failure of a fingerprint identification system when it does not match a candidate fingerprint pattern with its mating fingerprint pattern (in other words, a failure to make a match that should have been made).

Type II Error

The failure of a fingerprint identification system when it matches a candidate fingerprint pattern with a non-mating fingerprint pattern (in other words, making a match that should not have been made)

Validation

The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification

A comparison of two sets of biometrics to determine if they are from the same individual; or, in fraud prevention applications, a one-to-one comparison of a live finger and a previously enrolled record to ensure that the applicant is who he/she claims to be.

Source: I/O Software, Inc., 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. BIOMETRIC PRODUCTS AND APPLICATIONS

Company	Products
IrisScan Inc., U.S.A.	• IrisScan 2020 • System 2000 EAC • System 2100
Sensar, U.S.A.	• IrisIdent System
Panasonic, U.S.A.	• Authenticam

Table F.1. Iris Scanning Products. (After: Polemi, p. 24).

Company	Products
PrintScan International, U.S.A.	• WinFing 3.1
Startek, Tiawan	• FingerCheck
Identix, U.S.A.	• TouchPrint 600 • TouchPrint 2000 Live Scan System
Sony, Japan	• FIU-710 “Puppy” Fingerprint ID unit
Precise Biometrics, U.S.A.	• SC-100, MC-100, A-100 • BioKeyboard 100, • BioAccess MC, BioAccess Mifare
FingerScan, Australia	• FingerScan
FingerMatrix, U.S.A.	• FingerScanner
Bioscrypt, Canada	• V-Pass, V-Flex, V-Prox, V-Smart • MV 1200, Core
AuthenTec, Inc., U.S.A.	• EntrePad AES3500
Biocentric Solutions, Inc., U.S.A.	• BioSentry
BioEnable Technologies, India	• BioEnable FRT
BioPay, LLC, U.S.A.	• BioPay Check Cashing System
Bioscrypt, Inc., U.S.A.	• V-Smart
Cansec Systems Ltd., U.S.A.	• Zodiac Fingerprint Reader
DitigalPersona, Inc., U.S.A.	• U.are.U Pro
Fujitsu Microelectronics America, Inc., U.S.A.	• MBF300 Sweep Sensor
Global Biometric Corporation	• ID Plus Token
IDynta Systems, Inc., U.S.A.	• BioLink Products
NEC Technologies, Inc., U.S.A.	• TouchPass
Printrak (Motorola), U.S.A.	• Omnitrak 8.0 AFIS/Palmprint Identification Technology
Raytheon, U.S.A.	• IDENT
Visionics, U.S.A.	• FingerPrinter CMS
SENSE Holdings, Inc., U.S.A.	• BioClock

Table F.2. Fingerprint Recognition Products. (After: Polemi, p. 23 and BiometriTech, 26 Mar 2002).

Company	Products
Computer Data Systems, U.S.A	• Hand Geometry Readers
Recognition Systems, U.S.A.	• HandPunch • ID3D HandKey • Hand Geometry Readers
BioMet Partners, U.S.A.	• Digi-2
Biometric Security Systems, U.K	• BioDentity System
Biometrics, Inc, U.S.A.	• FastPass II
Talos Technology Inc, U.S.A.	• PG-2001
IDentiCard, U.S.A.	• Hand Geometry Reader

Table F.3. Hand Geometry Products. (After: Polemi, p. 27).

Company	Products
Dectel Security Systems, U.K.	• Facial Data Base Systems
Forensic Security Services, U.K.	• Thermace • VIAS
Technology Recognition Systems	• FR1000
Facial Reco Associates	• Sherlock Face Recognition
Identicator, U.S.A.	• Facial Search System
Lawrence Livermore National Laboratory, U.S.A.	• KEN
National University of Singapore	• FACEit
George Mason University	• ARGUS
MIT Artificial Intelligence Laboratory	• Face Pass
UMIST	• FACE-SOM
University of Essex	• Facial Recognition Software
Dextel Security Systems, UK	• Dextel Crime Net
Identification Technologies International Inc., U.S.A	• One on One Facial Recognition Systems
ZN Security, Germany, Germany	• ZN-Face
NeuroMetric Vision Systems	• MufMaster
AcSys Biometrics Corporation, Canada	• AcSys FRS Entry • Acsys FRS Logon IT • AcSys FRS CoLo
BioDentity Systems Corporation, Canada	• SecureIDent
BioID America, Inc., U.S.A.	• Single Sign-on
Cognitec AG, U.S.A.	• Face VACS-Logon
GraphCo Technologies, Inc., U.S.A.	• Facetrac
Identico Systems, U.S.A.	• True ID
ImageWare Systems, Inc., U.S.A.	• Face ID
Imagis Technologies, Inc., Canada	• ID-2000
Neuridynamics Limited, U.K.	• Tridentity 3 Dimensional Face Recognition
Photo Vision, Inc., U.S.A.	• QuadHDTV Video Image Sensor
Visionics, U.S.A.	• FaceIt (Figure 5.15.)
Viisage Technology, Inc., U.S.A.	• FaceFINDER (Figure 5.16.) • Face EXPLORER • FacePASS, FacePIN, FaceTOOLS
Symtron Technology, U.S.A.	• FaceOn Logon System • FaceOn Surveillance System

Table F.4. Facial Recognition Products. (After: Polemi, p. 25 and BiometriTech, 15 May 2002).

Company	Products
ABS, Germany	• VOCAL • VOCAL SCW1 • VOCAL ZKE
T-NETIX, U.S.A.	• PIN-LOCK, voice verification system
Bell Security, U.K.	• Caller Verification System
Speakez, U.S.A.	• Tele-MAtic
Domain Dynamic Limite, UK	• TESPAR/FANN
Anovea Authentication Technology, Inc., U.S.A.	• Anovea Speaker Authentication System
BioID America, Inc., U.S.A.	• BioID 3.0
Buytel (VoiceVault), Ireland	• Voice Vault Services
InterVoice-Brite, Inc., U.S.A.	• Speech Access
Keyware, U.S.A.	• Centralized Authentication Software (CAS)
Nuance Communications, U.S.A.	• Nuance Verifier 3.0
OTG, Canada	• HELP YOURSELF/SecurPBX
Persay Ltd., U.S.A.	• Orpheus
Sonic Foundry, Inc., U.S.A.	• Unified Security View
SpeechWorks International, Inc., U.S.A.	• SpeechSecure
SpeakEZ, U.S.A.	• Voice Print Speaker Verification SDK
Veritel Corporation	• VoiceCheck
VeriVoice, Inc., U.S.A.	• VeriVoice Security Lock (SL)
Vocent Solutions, Inc., U.S.A.	• Voice Secure Suite

Table F.5. Voice Recognition Products. (After: Polemi, p. 29 and BiometriTech, 1 Mar 2002).

Company	Products
Communication Intelligence Corp., U.S.A	• Signature Verification Software
Gadix, U.S.A.	• Cyber-SIGN
Quintet, U.S.A.	• Electronic Signature Verification System
British Technology Group, U.K.	• Rolls Royce Signature Verification
PenOp Inc., U.S.A.	• Signature Analyzer
AEA Technology, U.K.	• Countermatch
cadix International, Japan	• ID-007
IBM. U.S.A.	• IBM Transaction Security System
Checkmate Electronice, U.S.A.	• Sign/On

Table F.6. Handwriting/Signature Recognition Products. (After: Polemi, p. 30).

Company	Products
BioPassword Security Systems, U.K.	• BioPassword
Electronic Signature Lock Corporation, U.S.A.	• Electronic Signature Lock
M&T Technologies, U.S.A.	• Keystroke Analyzer
TNO-FEL, Netherlands	• Keystroke Analyzer

Table F.7. Keystroke Analysis and Recognition Products. (After: Polemi, p. 30).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. BIOMETRIC APPLICATIONS

• Correction Facilities	• Health Records Management
• Department of Motor Vehicles	• Secure Records Management
• Computer Login Validation	• Internet Automated Banking
• Corporate Domain Logon	• Credit Card Authorization
• ATMs	• Portal Entry Control
• Nuclear Power Station Security	• Electronic Commerce Security

Table G.1. Iris Scanning Applications. (From: Polemi, p. 24).

• Physical Access Control	• Banking
• Government Agencies	• Information Security
• Medical & Insurance Industry	• Police Department
• High Power Reactor Stations	• Immigration and Naturalization Services
• Airport Traffic Security	• Welfare & Unemployment Benefit Recipients
• Identification of Missing Children	• Database management systems
• Computer access or transaction control	• Computer Database Security Control

Table G.2. Fingerprint Recognition Applications. (From: Polemi, p. 23).

• Airport Traffic	• Banking
• Immigration and Naturalization Services	• Employee Verification
• Time and Attendance	• Super Markets
• Hospitals/Medical Security	• Drug Stores
• Stock rooms/Equipment Storage	• Computer Room Access
• Power Stations	• Welfare
• Casinos (access to money rooms)	• Prison Visitor/Inmate Control
• Universities/Research Laboratories	

Table G.3. Hand Geometry Applications. (From: Polemi, p. 26)

• Banking	• Credit Card Companies
• Airport Security	• Security of Internet
• Welfare Agencies	• Buildings Security
• Computer Facilities	• Drivers Licenses
• Telephone Companies	• Voter Registration Processes
• Hospitals/ Health Care Institutions	• Social Security Systems
• Police Authorities	• Vehicle Safety

Table G.4. Facial Recognition Applications. (From: Polemi, p. 25).

• Anti theft systems for vehicles and doors	• Telephone Networks
• PC and computer network access control	• Passport control
• Door entrance systems	• Prison Payphones
• Hospitals (access to nursery)	• Pharmacy
• Benefit Payments	• Aerospace company
• Equipment to authorize chip and magnetic key cards	• Fraud Control in prisons and correction facilities
• Universities (access to laboratories, computer centers, student unions)	• Air Force in air communications (identify pilots)
• Enforcement of bail	• Non custodial activities

Table G.5. Voice Recognition Applications. (From: Polemi, p. 28).

• Banking	• Internal Revenue Service
• Post Office	• Social Medicare
• Home Shopping	• Welfare

Table G.6. Handwriting/Signature Recognition Applications. (From: Polemi, p. 30).

LIST OF REFERENCES

123CCTV.com, "Security Camera Surveillance Equipment," 123CCTV.com, 2002, Available Online, [http://www.123cctv.com/], 123CCTV.com, Jun 2002.

Adams, James, "The Next World War – Computers are the Weapons & the Front Line is Everywhere," Simon & Schuster, 1998.

Amato, Ivan, "Big Brother Logs On," Technology Review Magazine, pp. 58-63, Vol. 104, No. 7, Sep 2001.

American Management Association (AMA), "Electronic Monitoring and Surveillance," 2002, Available Online, [http://www.amanet.org/research/emssurvey.htm#addendum], amanet.org, Mar 2002.

Analsphere.com, "The Costs of Freedom?" 21 May 2001, Available Online, [http://www.analysphere.com/21May01/costs.htm], Analsphere.com, Oct 2001.

Ancore Corporation, "Advanced Security and Inspection Company Ancore Applauds Bush Effort to Combat Terrorism: Asks New Office of Homeland Security to Focus Quickly on Solutions to Terrorist Threats," Ancore Corporation Press Releases, 25 Sep 2001, Ancore.com, May 2002.

Ancore Corporation, "Customs Aviation Security Bill Mandates Need for Luggage and Cargo Screening, Hazardous Material Detection," Ancore Corporation Press Releases, 19 Nov 2001, Ancore.com, May 2002.

Ancore Corporation, "Customs Service, DOD to Test PFNA Neutron Scanning at U.S. Border Crossing: Neutron Scanners Can Detect All Forms of Explosives Including Components for Dirty Bombs," Ancore Corporation Press Releases, 19 Mar 2002, Ancore.com, May 2002.

Ancore Corporation, "New Weapons Against Terrorism: Neutron Scanning Technologies Detect All Forms of Explosives Including Chemical Weapons, Liquid Explosives," Ancore Corporation Press Releases, 11 Oct 2001, Ancore.com, May 2002.

Ancore.com, "Products," Ancore.com, 2002, Available Online, [http://www.ancore.com/products.htm], Ancore.com, Jun 2002.

ANSER, "What Is Homeland Security? A Short History," Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/bulletin/ActionPlan_WhatIsHLS.htm], homelandsecurity.org, 28 Feb 2002.

ANSER, S.1214 - “The Port and Maritime Security Act of 2001,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1429 - “Airport and Seaport Terrorism Prevention Act,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1447 - “Aviation and Transportation Security Act,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1510 - “Uniting and Strengthening America Act (USA Patriot Act of 2001),” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1520 - “State Bioterrorism Preparedness Act,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1534 - “Department of National Homeland Security Act of 2001,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1602 - “Chemical Security Act of 2001,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.1715 - “Bioterrorism Preparedness Act of 2001,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

ANSER, S.R.165 - “Establishing a Select Committee on Homeland Security and Terrorism,” Analytic Services Inc., 2002, Available Online, [http://www.homelandsecurity.org/leg_update/index.cfm], homelandsecurity.org, Mar 2002.

Arena, Kelli and Lewandowski, Beth, “FAA Didn't Warn Airlines about Moussaoui,” CNN, 20 May 2002, Available Online, [http://www.cnn.com/2002/LAW/05/20/inv.moussaoui.warning/index.html], CNN.com, 21 May 2002.

Army-Technology.com, “Predator Unmanned Aerial Vehicle, USA,” Army-Technology.com, 2002, Available Online, [http://www.army-technology.com/predator], Army-Technology.com, Jul 2002.

Arnot, Bob, "Air Patrols Cast Dragnet on High Seas: Ships Watched for al Qaeda on the Run," MSNBC, 14 Mar 2002, Available Online, [http://www.msnbc.com/news/723992.asp?0dm=B327N], MSNBC.com, Jun 2002.

Arquilla, Electronic Correspondence between Dr. John Arquilla, Associate Professor, Department of Defense Analysis at Naval Postgraduate School, Monterey, CA and the Authors, 4 Apr 2002.

Arquilla, John and Ronfeldt, "Networks and Netwars," RAND National Defense Research Institute, 2001.

Arquilla, John, and David Ronfeldt, "Fight Networks with Networks," RAND Review, Dec 2001, Available Online, [http://www.rand.org/publications/randreview/issues/rr.12.01/], RAND.org, Jun 2002.

Ashbourn, Julian, "Biometrics: Advanced Identity Verification," Springer-Verlag, London, Great Britain, 2000.

Associated Press, "Bomb-Sniffing Dogs Prepare for Airport Duty," Associated Press, 7 Apr 2002, America Online, Apr 2002.

Associated Press, "Global Hawk Spy Drone Grounded," Associated Press, 12 Jul 2002, Available Online, [http://www.msnbc.com/news/779782.asp?0dm=C25EN], MSNBC.com, Jul 2002.

Associated Press, "INS Site to Track Foreign Students," Associated Press, 2 Jul 2002, Available Online, [http://www.msnbc.com/news/775479.asp?0dm=C25PN], MSNBC.com, Jul 2002.

Associated Press, "U.S. Delivers Copters to Pakistan," Associated Press, 5 Jul 2002, Available Online, [http://www.nytimes.com/aponline/international/AP-Pakistan-US..html], NYTimes.com, Jul 2002.

Associated Press, "U.S. to Increase Airport Patrols," MSNBC.com, 6 Jul 2002, Available Online, [http://www.msnbc.com/news/776641.asp], MSNBC.com, Jul 2002.

Atkinson, Robert D., and Ham, Shane, "Modernizing the State Identification System," Progressive Policy Institute, 7 Feb 2002, Available Online, [http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecid=290&contentid=250175], ppionline.org, Mar 2002.

Atkinson, Robert D., and Ham, Shane, "Using Technology to Detect and Prevent Terrorism," Progressive Policy Institute, 18 Jan 2002, Available Online, [http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=124&subsecid=307&contentid=250070], ppionline.org, Mar 2002.

Avid, “Forensic Tools from Avid An Ocean Systems,” Avid Technology, Inc. 2000-2002, Available Online, [http://www.avid.com/products/forensic/], Avid.com, Jun 2002.

Balaban, Dan, “Biometrics Touch Down at Major Airports,” Card Technology Magazine, 3 Jun 2002, Available Online, [http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20020603CTMN563.xml/], CardTechnology.com, Jun 2002.

Banisar, David, “Labour Pains: the Birth of a Movement,” Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss9.htm] UNESCO.org, Oct 2001.

Barrett, Jennifer, “Banking on Software Solutions,” Newsweek, 12 Jun 2002, Available Online, [http://www.msnbc.com/news/766013.asp], MSNBC.com, Jul 2002.

Barrett, Steve, “Transforming the Forces,” The Retired Officer Magazine, pp. 72-82, Vol. LVIII, No. 4, Apr 2002.

BBC, “Big Brother Cameras to Fight Crime,” 21 Aug 2001, Available Online, [http://news.bbc.co.uk/hi/english/uk/wales/newsid_1502000/1502034.stm], BBC News, 10 May 2002.

BBC, “CCTV Cameras Go Domestic,” 8 Nov 2001, Available Online, [http://news.bbc.co.uk/hi/english/uk/england/newsid_1644000/1644559.stm], BBC News, 10 May 2002.

BBC, “Experts Check Passport Changes,” 21 Feb 2002, Available Online, [http://news.bbc.co.uk/hi/english/sci/tech/newsid_1833000/1833939.stm], BBC News, 10 May 2002.

BBC, “More CCTV Cameras to Fight Crime,” 21 Aug 2001, Available Online, [http://news.bbc.co.uk/hi/english/uk/newsid_1501000/1501533.stm], BBC News, 10 May 2002.

BBC, “New CCTV for Vandal-hit Metro,” 11 Jan 2002, Available Online, [http://news.bbc.co.uk/hi/english/uk/england/newsid_1754000/1754138.stm], BBC News, 10 May 2002.

Behr, Mary E., “Biometrics to Get an XML Standard,” PC Magazine, 18 Mar 2002, Available Online, [http://www.pcmag.com/print_article/0,3048,a=24184,00.asp/], PCMag.com, Jun 2002.

Bhambhani, Dipka, “4 Million at DoD to Use Biometrics,” Government Computer News (GNC), pp. 1 and 8, 6 May 2002.

Bhambhani, Dipka, “Agencies Don’t Buy Biometrics Yet,” Government Computer News, p. 8, Vol. 21, No. 7, 1 Apr 2002.

Bhambhani, Dipka, "Patriot Law Put Federal Eye on Biometric Use," Government Computer News, pp. 1 and 10, 3 Jun 2002.

Bhambhani, Dipka, "What's Wrong with These Pictures?" Government Computer News, 15 Jul 2002, pp. 1 and 10.

"Big Brother - Watching in Britain," 13 Aug 2001, Available Online, [http://www.msnbc.com/news/613287.asp], MSNBC/Reuters Limited, Sep 2001.

Bigun, Josef; Borgefors, Gunilla and Chollet Gerard, "Audio and Video Based Person Authentication" (AVBPA), Lecture Notes in Computer Science - Conference Proceedings, Springer-Verlag Berlin Heidelberg, 1997.

BioConsulting, "Biometric Technical Assessment," BioConsulting.com, 5 May 2001, Available Online, [http://www.bioconsulting.com/Bio_Tech_Assessment.html/], BioConsulting.com, Jun 2002.

BiometriTech, "Facial-Recognition Solutions Roundup," BiometriTech, 15 May 2002, Available Online, [http://www.biometritech.com/features/roundup051502.htm], BiometricTech.com, Jun 2002.

BiometriTech, "Fingerprint Identification Roundup," BiometriTech, 26 May 2002, Available Online, [http://www.biometritech.com/features/roundup032602.htm], BiometricTech.com, Jun 2002.

BiometriTech, "Voice Identification and Authentication Roundup," BiometriTech, 1 May 2002, Available Online, [http://www.biometritech.com/features/roundup030102.htm], BiometricTech.com, Jun 2002.

BiometriTech.com, "Safe-Travel Ready To Launch Secure Perimeter Identification System," BiometriTech News, 5 Aug 2002, Available Online, [http://www.biometritech.com/enews/080502a.htm], BiometriTech.com, Aug 2002.

BiometriTech.com, "Visage Announces Casino, Submarine Base Deployments," BiometriTech News, 8 Jul 2002, Available Online, [http://www.biometritech.com/enews/070802f.htm], BiometriTech.com, Jul 2002.

Blackburn, Duane, "Facial Recognition 101," 10 Aug 2001, Available Online, [http://www.dodcounterdrug.com/facialrecognition/], Feb 2002.

Bougon, Yves and Temman, Michel, "Japan: Voyeuristic Games," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss3.htm] UNESCO.org, Oct 2001.

Boukhari, Sophie and Otchet, Amy, "They're Watching You: Privacy in a Wired World," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss0.htm], UNESCO.org, Oct 2001.

Bridis, Ted, "U.S. Unveils Anti-Terror Visa Plan," Associated Press, 6 Jun 2002, America Online News, Jun 2002.

Brown, Douglas R., Ph. D, Vice President for Business Development and Programs, Ancore Inspection Technologies, "Prepared Statement: Hearing on Implementation of S. 1214, The Port and Maritime Security Act of 20001," Committee on Commerce, Science and Transportation, U.S. Senate, Charleston Maritime Center, Charleston, SC, 19 Feb 2002.

Brown, Robert M., "The Electronic Invasion," Hayden Book Company Inc., 1975.

Bureau of Justice Statistics, "Key Crime & Justice Facts at a Glance," 10 Feb 2002, Available Online, [http://www.ojp.usdoj.gov/bjs/glance.htm], USDOJ.gov, 10 May 2002.

Cameron, David, "Walk This Way," Technology Review, 23 Apr 2002, Available Online, [http://www.technologyreview.com/articles/print_version/wo_cameron042302.asp/], TechnologyReview.com, May 2002.

Campbell, Duncan, "Shhh... They're Listening," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss10.htm] UNESCO.org, Oct 2001.

Card Technology Magazine, "Biometric Data Stored on Smart Cards Limits Spoofing," Card Technology Magazine, 18 Jun 2002, Available Online, [http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20020618CTDN701.xml/], CardTechnology.com, Jun 2002.

Card Technology Magazine, "U.S. Transport Worker Chip Card Coming Soon, Consumer Card to Follow," Card Technology Magazine, 12 Jun 2002, Available Online, [http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20020612CTDN650.xml/], CardTechnology.com, Jun 2002.

CardTechnology.com, "UK Government Floats Idea For National ID Card," Card Technology, 8 Jul 2002, Available Online, [http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20020708CTDN068.xml], CardTechnology.com, Jul 2002.

CardTechnology.com, "University Campus To Use Biometrics," Card Technology, 9 Jul 2002, Available Online, [http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20020709CTDN089.xml], CardTechnology.com, Jul 2002.

CardTechnology.com, "Virginia Beach Tries Facial Recognition To Spot Criminals, Runaways," Card Technology, 3 Jul 2002, Available Online, [http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20020703CTDN033.xml], CardTechnology.com, Jul 2002.

Cass, Stephen, "Improving Security, Preserving Privacy," IEEE SPECTRUM, Vol. 39, No. 1, Jan 2002.

Caterinicchia, Dan, “Army MPs Go Biometric,” Federal Computer Week, pp. 13, Vol. 16, No. 7, 18 Mar 2002.

CBSNews.com, “U.S. Cyberspace Still At Risk,” CBSNews.com, 23 Jul 2002, Available Online, [http://www.cbsnews.com/stories/2002/07/23/tech/printable516004.shtml], CBSNews.com, Jul 2002.

Center for Democracy and Technology: Overview of Response to FBI CALEA Implementation Plan - Industry and Privacy Advocates Response, Available Online, [http://www.cdt.org/digi_tele/970429_resp_over.html], cdt.org, 29 Apr 1997.

Chidambaram and Zigurs, “Our Virtual World: The Transformation of Work, Play and Life via Technology,” Idea Group Publishing; 2001.

Cho, Aileen, “Airlines Are Clearing a Nonstop Path to the Plane,” The New York Times, 5 Aug 2001, [http://www.nytimes.com/2001/08/05/technology/05AIRP.html]. Sep 2001.

CNN, “Airline Security: Congress Passes Compromise Bill,” CNN, 17 Nov 2001, Available Online, [http://www.cnn.com/2001/US/11/17/rec.airport.security.facts/index.html], CNN.com, Mar 2002.

CNN, “An FBI Field Agent,” CNN, 20 May 2002, Available Online, [http://www.cnn.com/2002/ALLPOLITICS/05/20/time.fieldagent/index.html], CNN.com, 21 May 2002.

CNN, “Cheney: 'No Doubt' Terrorists Wish to Strike Again,” CNN, 24 May 2002, Available Online, [http://www.cnn.com/2002/ALLPOLITICS/05/24/cheney.navy.grad/index.html], CNN.com, 25 May 2002.

CNN, “FBI Chief: We Will Not Be Able to Stop It,” CNN, 20 May 2002, Available Online, [http://www.cnn.com/2002/US/05/20/gen.war.on.terror/index.html], CNN.com, 21 May 2002.

CNN.com, “Future of Spying: Tiny Flying Bots,” CNN.com, 28 Jul 2002, Available Online, [http://www.cnn.com/2002/TECH/science/07/28/flying.micro.bots.ap/index.html], CNN.com, Jul 2002.

Cohen, Tom, “Canada, U.S. Agree on ‘Smart Border’ Plan,” Times Argus, 21 Jun 2001, Available Online, [http://www.timesargus.nybor.com/Story/39116.html/], Timesargus.com, Jun 2002.

Collins, Sharon, “Trading PINs for Body Parts,” CNN, 18 Aug 2000, [http://www.cnn.com/2000/TECH/computing/08/18/biometrics/index.html], Sep 2001.

Crewdson, John and Tom Hundley, “al Qaeda ‘Sleepers’ May Be in U.S.: Italy’s Eavesdropping on Terrorists Hints at Infiltration beyond Sept. 11 Group,” Chicago Tribune, 30 Jun 2002, Available Online, [http://www.chicagotribune.com/news/nationworld/showcase/chi-0206300380jun30.story?coll=chi%2Dnews%2Dhed], ChicagoTribune.com, Jun 2002.

Daukantas, Patricia, “DOD Biometrics Lab Looks to Expand,” Government Computer News, 15 Jul 2002, p. 10.

Daukantas, Patricia, “Feds Focus on Biometric Tools,” Government Computer News, pp. 1 & 12, Vol. 21, No. 8, 15 Apr 2002.

Davies, Simon, “And the Spy Who Loves Us All,” Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss2.htm] UNESCO.org, Oct 2001.

Davies, Simon, “The Spy in your Refrigerator,” Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss1.htm] UNESCO.org, Oct 2001.

Davis, M. Thomas, “Homeland Security: New Mission of a New Century,” Northrop Grumman Corporation, Jan 2002, Available Online, [http://www.capitol.northgrum.com], 2 Apr 2002.

Davis, Shelley, “Fighting Bioterror,” The Retired Officer Magazine, pp. 56-62, Vol. LVIII, No. 4, Apr 2002.

Delio, Michelle, “Privacy Advocate Shifts Gears,” Wired News, 8 Nov 2001, Available Online, [http://www.wired.com/news/exec/0,1370,48197,00.html], wired.com, Mar 2002.

DeNoon, Daniel, “Liar, Liar, Face on Fire,” AOL Health, 25 Jun 2002, AOL, Jun 2002.

DePersia, A. Trent, Yeager, Suzan and Ortiz, Steve, “Surveillance and Assessment Technologies for Law Enforcement,” Proceedings: SPIE-The International Society for Optical Engineering, Vol. 2935, Nov 1996.

Diamond, John, “Arab Spelling Slows Inquiries in Terror War,” USA Today, 1 Jul 2002, Available Online, [http://www.usatoday.com/news/attack/2002/06/30/arab-spelling.htm], USAToday.com, Jul 2002.

Dixon, Patrick, “Are You Being Bugged?” 2002, Available Online, [http://www.globalchange.com/bug.htm], Globalchange.com, Mar 2002.

Dizard III, Wilson P., “INS Speeds Makeover of Visa Systems,” Government Computer News, pp. 1 & 12-13, Vol. 21, No. 7, 1 Apr 2002.

Dizzard III, Wilson P., “Can INS Handle Alien Entry Plan?” Government Computer News, 17 Jun 2002, p. 15.

Dizzard III, Wilson P., "Challenge No. 2: Set an Overachieving System Agenda," Government Computer News, 17 Jun 2002, p. 13.

DOE Human Genome Project, "DNA Details," ORNL.gov, Available Online, [http://www.ornl.gov/hgmis/graphics/slides/genetalk.html/], ORNL.gov, May 2002.

Dorobek, Christopher J., "A New Plan of Attack," Federal Computer Week, pp. 18-21, Vol. 16, No. 6, 11 Mar 2002.

Doyle, Rodger, "Privacy in the Workplace," Scientific American, 1999, Available Online, [http://www.sciam.com/1999/0199issue/0199numbers.html], sciam.com, Mar 2002.

Dreyfus, Suelette, "The Quiet Revolution," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss6.htm] UNESCO.org, Oct 2001.

Driggers, Ronald G. and Leachtenauer, Jon C., "Surveillance and Reconnaissance Imaging Systems – Modeling and Performance Prediction," Artech House Inc., 2001.

Dysart, Aidan, "Biometrics," University of Michigan, EECS 598, Winter 1998, Available Online, [http://www.monkey.org/~aidan/598/], Monkey.org, May 2002.

Eggen, Dan, "Airports Screened Nine of Sept. 11 Hijackers, Officials Say," Washington Post, 2 Mar 2002, p. A11.

Electronic Privacy Information Center (EPIC), "National ID Cards," EPIC, Available Online, [http://www.epic.org/privacy/id_cards/], Epic.org, Jun 2002.

Elliott, Michael, "How the U.S. Missed the Clues," CNN, 20 May 2002, Available Online, [http://www.cnn.com/2002/ALLPOLITICS/05/20/time.clues/index.html], CNN.com, 21 May 2002.

Ellis, Kathleen, "ID Them By the Way They Walk," Wired News, 15 Sep 2000, Available Online, [http://www.wired.com/news/print/0,1294,38775,00.html], Wired.com, Jun 2002.

Emerson, Steven, "American Jihad – The Terrorist Living Among Us," The Free Press - A Division of Simon & Schuster Inc., 2002.

Encarta, "Biometrics," Microsoft, Available Online, [http://encarta.msn.com/encarta/], Encarta.MSN.com, Jun 2002.

EyeTicket Corporation, "Airline Ticketing, Check-In and Boarding," "Aviation Access Control," "Sports and Entertainment Admissions," McLean, VA, 2001, [http://www.eyeticket.com], Sep 2001.

FAS, “Predator UAV Product,” FAS, 22 Jun 1996, Available Online, [http://www.fas.org/irp/imint/predator.htm], FAS.org, Jul 2002.

Fialka, John J., “U.S. Nuclear Plants Differ on Security: Widespread Squabbling Delays a National Plan,” The Wall Street Journal, 3 Jul 2002, Available Online, [http://www.msnbc.com/news/775738.asp?0bl=-0], MSNBC.com, Jul 2002.

Fish, Mike, “Airport Security: A System Driven by the Minimum Wage,” CNN, 2002, Available Online, [http://www.cnn.com/SPECIALS/2001/trade.center/flight.risk/stories/part1.mainbar.html], CNN.com, 28 Feb 2002.

Frank, Diane, “Bush Seeks Security Budget Boost,” Federal Computer Week, p. 6, Vol. 16, No. 8, 25 Mar 2002.

Frank, Diane, “Homeland Threat System Released,” Federal Computer Week, p. 50, Vol. 16, No. 7, 18 Mar 2002.

Froomkin, Michael A., “The Death of Privacy?” University of Miami School of Law, 1 Feb 2000, Available Online, [http://personal.law.miami.edu/~froomkin/articles/privacy-deathof-text.htm], Oct 2001.

Future Harvest, “Harvest for People,” 8 May 2002, Available Online, [http://www.futureharvest.org/people/background.shtml], futureharvest.org, 16 May 2002.

GAO, GAO-01-1158T, “Homeland Security: A Framework for Addressing the Nation's Efforts General,” 21 Sep 2001, Available Online, [http://www.gao.gov], General Accounting Office, Apr 2002.

Garson, David, G., “Social Dimensions of Information Technology,” Idea Group Publishing; 2000.

Gates, Robert, M., “A Former CIA Chief on ‘Connecting the Dots’...,” CNN, 20 May 2002, Available Online, [http://www.cnn.com/2002/ALLPOLITICS/05/20/time.chief/index.html], CNN.com, 21 May 2002.

GCN, “Systems Will Range from Data Centers to Biometrics,” Government Computer News, 24 Jun 2002, p. 16.

Gellman, Barton, “Cyber-Attacks by al Qaeda Feared,” The Washington Post, 27 Jun 2002, Available Online, [http://www.msnbc.com/news/772908.asp?0dm=C27KN], MSNBC.com, Jun 2002.

Gilot, Louie, "Customs Buys 'Dirty Bomb' Detectors," El Paso Times, 27 Jul 2002, Available Online, [http://www.elpasotimes.com/stories/business/20020727-5160.shtml], El PasoTimes.com, Aug 2002.

Gomes, Lee, "Can Facial Recognition Help?" The Wall Street Journal, 27 Sep 2001, Available Online, [http://www.msnbc.com/news/634892.asp], MSNBC.com, Sep 2001.

Gozani, Tsahi, Ph. D, P.E., Chief Executive Officer and President, Ancore Corporation, "Prepared Statement: Hearing on Role of Military Research and Development Programs in Homeland Security," Committee on Armed Services Subcommittee on Research and Development, House of Representatives, Washington, District of Columbia, 12 Mar 2002.

Graham, Stephen, "News & Analysis The Privacy Issue: The Fifth Utility," Issue 3, 2000, Available Online, [http://www.oneworld.org/index_oc/300/gra.htm], Index Online, Oct 2001.

Gray, Chris H., "Postmodern War – The New Politics of Conflict," The Guilford Press, 1997.

Greenman, Catherine, "In the Airport Fast Lane, With Your Eyes as a Passport," The New York Times, 2 Aug 2001, [http://www.nytimes.com/2001/08/02/technology/circuits/02NEXT.html], Sep 2001.

Greenman, Catherine, "Tracking an Outbreak Minute by Minute," The New York Times, 4 Jul 2002, Available Online, [http://www.nytimes.com/2002/07/04/technology/circuits/04SICK.html], NYTimes.com, Jul 2002.

Guevin, Laura, "A Compilation of Biometric Case Studies," BiometriTech, 9 April 2002, Available Online, [http://www.biometritech.com/features/deploywp6.htm], BiometricTech.com, Jun 2002.

Gunaratna, Rohan, "Inside al Qaeda: Global Network of Terror," New York: Columbia University Press, 2002.

Haddock, Vicki, "Loose Nukes A Radioactive "Dirty Bomb" Could Be Headed for your Neighborhood," San Francisco Chronicle, 28 Apr 2002, Available Online, [http://www.nci.org/index.htm], NCI.org, 26 May 2002.

Ham, Shane and Robert D. Atkinson, "Modernizing the State Identification System: An Action Agenda," Progressive Policy Institute, Policy Report, Feb 2002, Available Online, [http://ppionline.org/], PPIOnline.org, May 2002.

Hanson, Judi, "Bush Delivers Homeland Blueprint," Federal Computer Week, 19 Jun 2002, Available Online, [http://www.fcw.com/fcw/articles/2002/0617/web-bill-06-19-02.asp], FCW.com, Jun 2002.

Harreld, Heather, "Biometrics Points to Greater Security," Federal Computer Week, 19 Jul 2002, Available Online, [http://www.fcw.com/print.asp/], FCW.com, Jun 2002.

Harris, Shane, "Bureaucratic Battles Bog Down Biometrics," Government Executive Magazine, 1 Jan 2002, Available Online, [http://www.govexec.com/features/0102/0102managetech1.htm/], GovExec.com, Jun 2002.

Hasson, Judi, "Bush Delivers Homeland Blueprint," Federal Computer Week, 19 Jun 2002, Available Online, [http://www.fcw.com/fcw/articles/2002/0617/web-bill-06-19-02.asp/], FCW.com, Jun 2002.

Hasson, Judi, "Priming the Pump: Companies Prep Slew of Homeland Security Solutions, but Wait for Feds to Get the Money to Buy Them," Federal Computer Week, 1 Jul 2002, Available Online, [http://www.fcw.com/print.asp], FCW.com, Jul 2002.

Hasson, Judi, "Smart Building IDs Gaining Support," Federal Computer Week, p. 8, Vol. 16, No. 13, 29 Apr 2002.

HHS News, "HHS Provides New Aid To Cities For Disaster Preparedness," HHS News, 10 Jul 2002, Available Online, [http://www.hhs.gov/news/press/2002pres/20020710.html], HSS.gov, Jul 2002.

Hogan, Kevin, "Will Spyware Work?" Technology Review Magazine, pp. 43-47, Vol. 104/No. 10, Dec 2001.

Hoge Jr., James F., and Rose, Gideon, "How Did This Happen? Terrorism and the New War," PublicAffairs™ Reports, Member of Perseus Book Group, 2001.

Holmes, Jennifer and Pitts, Chip, "Liberty vs. Security: Drawing the Line," Liberty, pp. 19-20, p. 61, Vol. 16, No. 5, May 2002.

Hsu, Spencer S., "Video Surveillance Planned on Mall: Cameras to Be Installed by October in and Around All Major Monuments," Washington Post, 22 Mar 2002, p. B1.

Hsu, Spencer S., "Video Surveillance Planned on Mall," The Washington Post Company, 22 Mar 2002, [http://www.washingtonpost.com/wp-dyn/articles/A102-2002Mar21.html], washingtonpost.com, Mar 2001.

I/O Software, "Biometrics Explained," I/O Software, Available Online, [http://www.iosoftware.com/biometrics/methods.htm], IOSoftware.com, Jun 2002.

I/O Software, Inc., "Biometrics Glossary," About Biometrics, 2002, [http://www.iosoftware.com/biometrics/glossary.htm], 8 Jun 2002.

Identix.com, "Mobile Identification," Identix.com, 2002, Available Online, [http://www.identix.com/products/pro_mobile_ibis.html], Identix.com, Jul 2002.

"Interest in Face Scanning Grows," MSNBC/Reuters Limited, 18 Sep 2001, Available Online, [http://www.msnbc.com/news/630735.asp], Oct 2001.

Invision-tech.com, "Products," Invision Technologies, 2002, Available Online, [http://www.invision-tech.com/products/products.htm/], Invision-tech.com, Jun 2002.

ISIS, "Automatic Gait Recognition and Extraction at ISIS," University of Southampton, 9 Jan 2001, Available Online, [http://www.isis.ecs.soton.ac.uk/image/gait/research.php3], ISIS.uk, May 2002.

Jackson, William, "Border Security Law Requires Data Sharing, Visa Readers for Tracking Foreign Visitors," Government Computer News, p. 10, 3 Jun 2002.

Jackson, William, "Challenge No. 1: Mesh Disparate Databases and Apps," Government Computer News, 17 Jun 2002, p. 12.

Jackson, William, "Challenge No. 3: Decide Who Does What and Why," Government Computer News, 17 Jun 2002, p. 12.

Jackson, William, "Foolproof Access: DOD Sets a Timeline for Biometric Cards," Government Computer News, 22 Jun 2002, pp. 47-48.

Jaffe, Greg, "U.S. Sub Fleet in Danger of Overuse," Wall Street Journal, 26 Jun 2002, Available Online, [http://www.msnbc.com/news/772454.asp?0dm=C25BN], MSNBC.com, Jun 2002.

Jain, Anil K., "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, U.S.A., 1999.

Johnson, Alex, "Full Bag Scanning May Be Years Away: 'Bureaucracy' Makes Stopgap Measures All But Permanent," MSNBC, 26 Mar 2002, Available Online, [http://www.msnbc.com/news/726695.asp /], MSNBC.com, Jun 2002.

Jonietz, Erika, "Automatic Networks – Devices that Connect Themselves Could Change Networking," MIT Technology Review Magazine, pp. 20-21, Vol. 105, No. 4, May 2002.

Kelley, Jack, "Militants Wire Web with Links to Jihad," USA Today, 10 Jul 2002, Available Online, [http://www.usatoday.com/life/cyber/tech/2002/07/10/terrorweb.htm], USAToday.com, Jul 2002.

Klein, Edward, "We're Not Destroying Rights, We're Protecting Rights," Parade Magazine, pp. 4-6, 19 May 2002.

Kugler, Sara, "Visitor's Faces Scanned at New York Landmarks," Washington Post, 26 May 2002, p. A14.

Kushner, Harvey W., "Terrorism in America – A Structured Approach to Understanding the Terrorist Threat," Charles C. Thomas Publisher LTD, 1998.

Kwon, Sue, "Homeland Security Expo in San Jose," Available Online, [http://beta.kpix.com/news/local/2001/12/13/Homeland_Security_Expo_in_San_Jose.html/], Kpix.com, Jun 2002.

Leopold, George, "Biometric Technology Moves to Secure Center Stage," EE Times, 14 Feb 2002, Available Online, [http://www.eetimes.com/story/OEG20020214S0051/], EENews.com, Jun 2002.

Lesser, Roger and Megan Alderton, "The New Face of Aviation Security," RF Design, 1 Jan 2001, Available Online, [http://www.industryclick.com/magazinearticle.asp?magazinearticleid=138516/], Industryclick.com, Jun 2002.

Library of Congress, "H.R. 1292 Homeland Security Strategy Act of 2001," 29 Mar 2001, Available Online, [http://thomas.loc.gov/home/thomas.html], 30 May 2002.

Library of Congress, "H.R.3026 Office of Homeland Security Act of 2001," 18 Mar 2002, Available Online, [http://thomas.loc.gov/home/thomas.html], 30 May 2002.

Lind, Michael, "Solving the Privacy Puzzle," The New Leader, A Bimonthly of News Analysis and Opinion, pp. 15-17, Vol. LXXXV, No. 1, Jan/Feb 2002.

Lisagor, Megan, "Reinventing FEMA," Federal Computer Week, pp. 14-19, Vol. 16, No. 8, 25 Mar 2002.

Lodal, Jan M. and James J. Shinn, "Red-Teaming the Data Gap," Counsil on Foreign Relations, Independent Task Force on America's Response to Terrorism, 1 Apr 2002, Available Online, [http://www.cfr.org/public/resource.cgi?pub!4548], CFR.org, Jul 2002.

Loy, James M., Admiral and Ross, Robert G., Captain, USCG, "Global Trade: America's Achilles Heel," Analytic Services Inc., Feb 2002, Available Online, [http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=33], Defense Horizons, 12 Mar 2002.

Lyon, David and Zureik, Elia, "Computers, Surveillance, & Privacy," University of Minnesota Press, 1996.

Maddocks, Ralph, "Have Orwell's Predictions Come True?" Le Quebecois Libre, 9 Jan 1999, Available Online, [http://www.quebecoislibre.org/990109-6.htm], QuebecoisLibre.org, Jun 2002.

Madsen, Wayne, "The Business of the Watchers – Privacy Protections Recede as the Purveyors of Digital Security Technologies Capitalize on September 11," Multinational Monitor, pp. 18-22, Vol. 23, No. 3, Mar 2002.

Maniscalco, Paul M., and Christen, Hank T., "Understand Terrorism and Managing the Consequences," Prentice Hall, 2002.

Mann, Steve, "Privacy Issues of Wearable Cameras Versus Surveillance Cameras," 24 Feb 1995, Available Online, [http://wearcam.org/netcam_privacy_issues.html], wearcam.com, Mar 2002.

Manwaring, Max G., "…to Insure Domestic Tranquility, Provide for the Common Defense…," Papers from the Conference on Homeland Protection, Strategic Studies Institute – U.S. Army War College, Oct 2000.

Marsan, Carolyn Duffy, "Security Chief Details U.S. Cybersecurity Plans," Network World Fusion, 12 Mar 2002, Available Online, [http://www.nwfusion.com/cgi-bin/mailto/x.cgi/], NWFusion.com, Jun 2002.

Masterson, Ursula Owre, "Airports Seek Hi-Tech Security," MSNBC, 11 Mar 2002, Available Online, [http://www.msnbc.com/news/720856.asp], MSNBC.com, Jun 2002.

Masterson, Ursula Owre, "Airports Seek Hi-Tech Security: All Seeing Devices are on the Market, but at What Price to Privacy," MSNBC, 3 Apr 2002, Available Online, [http://www.msnbc.com/news/729756.asp], MSNBC.com, Jun 2002.

Matthews, William, "FBI Spyware Avoids Scrutiny," Federal Computer Week, p. 34, Vol. 16, No. 6, 11 Mar 2002.

Matthews, William, "House Assails INS System," Federal Computer Week, p. 34, Vol. 16, No. 8, 25 Mar 2002.

Matthews, William, "Identity Crisis: Proposed Legislation Renews Debate about a National ID Card," Federal Computer Week, p. 16, Vol. 16, No. 17, 27 May 2002.

Matthews, William, "INS Taps CSC for Verification System," Federal Computer Week, p. 10, Vol. 16, No. 9, 1 Apr 2002.

Matthews, William, "Ridge: Link Driver's Licenses, Visas," Federal Computer Week, pp. 8-9, Vol. 16, No. 7, 18 Mar 2002.

Maussion, Catherine, "Data-Swindlers: Gold Mining in the Badlands of E-Commerce," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss4.htm] UNESCO.org, Oct 2001.

McCullagh, Declan, "Bush Submits His Laws for War," Wired News, 20 Sep 2001.

McCullagh, Declan, and Polen, Ben, "DOJ's Already Monitoring Modems," Wired News, 28 Nov 2001, Available Online, [http://www.wired.com/news/privacy/0,1848,48711,00.html], wired.com, Mar 2002.

McIntire, David, "What Is Homeland Security? A Short History," ANSER Institute for Homeland Security, 2002, Available Online, [http://www.homelandsecurity.org/bulletin/actionplan_whatishls.htm], 8 Jun 2002.

McMichael, James M. and Michael S. Francis, "Micro Air Vehicles: Toward a New Dimension in Flight," DARPA, 7 Aug 1997, Available Online, [http://www.darpa.mil/tto/MAV/mav_auvsi.html], DARPA.mil, Jul 2002.

Meehan, Michael, "Iris Scans Take Off at Airports," ComputerWorld, 19 July 2000, [http://www.cnn.com/2000/TECH/computing/07/19/iris.scan.idg/index.html], Sep 2001.

Meeks, Brock, N., "Big Boss is Watching You," MSNBC, 7 Dec 2000, Available Online, [http://www.msnbc.com/news/498455.asp], Oct 2001.

Mendenhall, Preston, "Chilling Lessons at al-Qaida U.," MSNBC News, 27 Aug 2002, Available Online, [http://www.msnbc.com/news/695030.asp], MSNBC.com, Sep 2002.

Menke, Susan M., "At Its Core, a Systems Shake-Up: Bush's Homeland Security Department Proposal Calls for an Enterprise Architecture," Government Computer News, 17 Jun 2002, pp. 1 and 12.

Miller, Bill, "Outdated Systems Balk Terrorism Investigations: FBI, for Example, Couldn't Track Flight School Data," Washington Post, 13 Jun 2002, p. A12.

Miller, Jason, "Who Will Take IT Reins at New Department?" Government Computer News, 17 Jun 2002, pp. 1 and 14.

Moore, John, "Grinding for the Grid," Federal Computer Week, p. 22, Vol. 16, No. 7, 18 Mar 2002.

MSNBC, "Big Abu Sayyaf Battle Underway: Arroyo Says Philippine Troops, Rebels Clash in South," MSNBC News Services, 28 Jun 2002, Available Online, [http://msnbc.com/news/770275.asp?0dm=C24BN], MSNBC.com, Jun 2002.

Nanavati, Samir, Thieme, Michael, and Nanavati, Raj, "Biometrics: Identity Verification in a Networked World," John Wiley & Sons, Inc., U.S.A., 2002.

Newman, Rick, "My Security Begins at Home," Washington Post, 31 Mar 2002, p. B4.

NewsMax.com, "Fingerprint Scanning Called for by House Bill," NewsMax.com Wires, 6 Oct 2001, Available Online, [http://www.newsmax.com/cgi-bin/printer_friendly.pl/] NewsMax.com, Jun 2002.

Newton, Christopher, "Technology for Catching Liars," The Associated Press, 21 Jun 2002, AOL, Jun 2002.

Nieto, Marcus, "Public Video Surveillance: Is It An Effective Crime Prevention Tool?" California Research Bureau, CRB-97-005, June 1997, Available Online, [http://www.library.ca.gov/CRB/97/05/], California State Library, May 2002.

Noble, Ivan, "The Eye's Have It," 9 Aug 2001, Available Online, [http://news.bbc.co.uk/hi/english/sci/tech/newsid_1477000/1477655.stm], BBC News, 10 May 2002.

O'Hanlon, Michael, "Protecting the American Homeland: Governor Ridge's Unfinished Work," The Brooking Review, Summer 2002, Vol. 20, No. 3, pp. 13-16, Available Online, [http://www.brook.edu/press/REVIEW/summer 2002/0hanlon.htm], Brook.edu, Jul 2002.

O'Hara, Colleen, "SSA Testing Biometric Tech," Federal Computer Week, p. 17, Vol. 16, No. 6, 11 Mar 2002.

O'Harrow, Robert Jr., "In Terror War, Privacy vs. Security: Search for Illicit Activities Taps Confidential Data," Washington Post, 3 Jun 2002, p. A1.

O'Harrow, Robert Jr., "Intricate Screening of Fliers in Works," The Washington Post Company, 1 Feb 2002, [http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A5185-2002Jan31&notFound=true], washingtonpost.com, Mar 2001.

Observing Surveillance, "Observing Surveillance," Available Online, [http://observingsurveillance.org/], ObservingSurveillance.org, Jun 2002.

Office of the Secretary of State, "Patterns of Global Terrorism," 21 May 2001, Available Online, [http://www.usis.usemb.se/terror/index.html], May 2002.

OneWorld, "News and Analysis," 2002, Available Online, [http://www.oneworld.net/us/], oneworld.net, 16 May 2002.

Onley, Dawn S., "Uncle Sam Gets Tough on Rule Governing Info Assurance Buys," Government Computer News, 17 Jun 2002, pp. 1 and 16.

Orenstein, David, "How a Bomb Sniffer Works," Business 2.0, Nov 2001, Available Online, [http://business2.com/articles/mag/print/0,1643,17513,FF.html/], Business2.com, Jun 2002.

ORNL.gov, "Enclosed Space Detection System," ORNL, National Security Markets: Surveillance, Measurements, and Analysis, Available Online, [http://www2.ic.ornl.gov/pdf/progr-38.pdf/], ORNL. Gov, Jul 2002.

Orwell, George, "Nineteen Eighty-Four," Harcourt Brace and Company Inc., 1949.

Otchet, Amy, "Forsaking Genetic Secrets," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss7.htm] UNESCO.org, Oct 2001.

Patton, Susannah, "Putting the Pieces Together," 1 Feb 2002, Available Online, [http://www.darwinmag.com/read/020102/together.html], Darwin Magazine, 20 May 2002.

Paulson, Tom, "Virtual Images May Help Spot Real Threats," Seattlepi.com, 5 Aug 2002, Available Online, [http://www.msnbc.com/local/pisea/81355.asp?0dm=C22QN], MSNBC.com, Aug 2002.

Peckinpaugh, Carl, "National ID Card Debate," Federal Computer Week, p. 44, Vol. 16, No. 13, 29 Apr 2002.

Peterson, Julie K., "Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications," CRC Press LLC, Boca Raton, Florida, 2001.

PictureQuest, "Retina," Picture Quest, 2001, Available Online, [http://www.picturequest.com/include/info.bhtml?caption_id=723867/], PictureQuest.com, Jul 2002.

Polemi, Dr. Despina, "Biometrics Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of Areas Where They Are Most Applicable," Institute of Communication and Computer Systems, National Technical University of Athens, Apr 1997.

Porteus, Liza, "Homeland Security Depends on New Technologies, Ridge says," 24 Apr 2002, Available Online, [http://www.govexec.com/dailyfed/0402/042402td2.htm], GovExec.com, 30 Apr 2002.

Priest, Dana and Douglas Farah, "Hezbollah, al Qaeda Form Alliance, U.S. says," Washington Post Service, 30 Jun 2002, Available Online, [http://www.miami.com/mld/miamiherald/2002/06/30/news/world/3572549.htm], Miami.com, Jun 2002.

Privacy.org, "Airline Passenger Profiling System," 1 Feb 2002, Available Online, [http://www.privacy.org/article.php?sid=1003&mode=thread&order=0&thold=0], Privacy.org, Mar 2001.

Raikow, David, "Pick a Finger, Any Finger," eWeek, 12 March 2001, Available Online, [http://www.eweek.com/print_article/0,3668,a=11546,00.asp], eWeek.com, Jun 2002.

RAND, "Organizing for Homeland Security," RAND Issue Paper, 2002.

Reeve, Simon, "The New Jackals – Ramzi Yousef, Osama bin Laden and the Future of Terrorism," Northeastern University Press, 1999.

Regan, Thomas M. and Willox, Norman A. Jr., "Identity Theft: Authentication as a Solution Revisited," 2 Oct 2001, Available Online, [http://www.lexisnexis.com/hottopics/aoa/AuthenticationWhitePaper.pdf], National Fraud Center, 10 May 2002.

Reuters, "Laden Alive as of Late December: Report," The Times of India, 1 Jul 2002, Available Online, [http://timesofindia.indiatimes.com/articleshow.asp?art_ID=14604150], Jul 2002.

Reuters, "Driver Licenses May Get High-Tech Fix," MSNBC, 17 Feb 2002, Available Online, [http://www.msnbc.com/news/709629.asp], 15 May 2002.

Reuters, "Face-Recognizing System Set for Takeoff in Airports," USA Today, 24 Sep 2001, Available Online, [http://www.usatoday.com/life/cyber/tech/2001/09/24/face-scanning.htm/], USAToday.com, May 2002.

Reuters, "Facial Recognition Put to the Test," Special to CNET News.com, 16 May 2002, Avanta.

Robinson, Brian, "The Eye of the Storm," Federal Computer Week, pp. 20-24, Vol. 16, No. 8, 25 Mar 2002.

Rohrer, Finlo, "UK's Surveillance Dilemma," 27 Sep 2001, Available Online, [http://news.bbc.co.uk/hi/english/uk/newsid_1566000/1566875.stm], BBC News, 10 May 2002.

Rolwing, Rebecca, "Don't See the Password, Be the Password," Computer Privacy & Security, Smart Computing Magazine, pp. 11-14, Vol. 8, Issue 4, 2002.

Rosen, Jeffrey, "A Cautionary Tale for a New Age of Surveillance," 7 Oct 2001, Available Online, [http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.htm] The New York Times, Oct 2001.

Roush, Wade "Networking the Infrastructure," Technology Review Magazine, pp. 39-42, Vol. 104, No. 10, Dec 2001.

Roxborough, Ian, "The Hart-Rudman Commission and the Homeland Defense," Strategic Studies Institute, Sep 2001.

Rumsfeld, Donald, Secretary of Defense, "Quote from Town Hall Meeting at Nellis AFB," ANSER Institute for Homeland Security," Available Online, [http://www.homelandsecurity.org/quotes/quote.cfm?Authorid=25], 26 Mar 2002.

Samarajiva, Rohan, "A Privacy Divide?" Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/opinion.htm] UNESCO.org, Oct 2001.

Sarkar, Dibya, "Iowa Blocks False IDs," Federal Computer Week, p. 35, Vol. 16, No. 6, 11 Mar 2002.

Sarnoff, "Video Detective Workstation from PVT Enhances Images for Law Enforcement Use," Sarnoff News & Press Releases, 1 Apr 2002, Available Online, [http://www.sarnoff.com/news/index.asp?releaseID=78], Sarnoff.com, Jun 2002.

Scheeres, Julia, "Some Camera to Watch Over You," 5 Apr 2001, Available Online, [http://www.wired.com/news/business/0,1367,42794,00.html], Wired News, Oct 2001.

Scheeres, Julia, "ID Cards Are *de Rigueur* Worldwide," Wired News, 25 Sep 2001, Available Online, [http://www.wired.com/news/print/0,1294,47073,00.html], Wired.com, Jun 2002.

Scheeres, Julia, "Support for ID Cards Waning," Wire News, 13 Mar 2002, Available Online, [http://www.wired.com/news/print/0,1294,51000,00.html/], Wired.com, Jun 2002.

Schloss, Glenn, "A Tireless Troubleshooter," Mar 2001, Available Online, [http://www.unesco.org/courier/2001_03/uk/doss8.htm] UNESCO.org, Oct 2001.

Sciencenet, "Watch How You Walk," Sciencenet, December 1999, Available Online, [http://www.sciencenet.org.uk/slup/CuttingEdge/Dec99/walk.html], ScienceNet.org, Jun 2002.

Senate Document No. 106-27, "Analysis of Cases Decided by the Supreme Court of the United States to June 28, 2000," Analysis and Interpretation of the Constitution of the United States of America, 2000 Supplement, Available Online, [http://www.access.gpo.gov/congress/senate/constitution/toc.html], Congressional Research Service Library of Congress, Mar 2002.

Sensar, Inc., "About Sensar," Available Online, [http://home.earthlink.net/~founders/sensar1.htm], Earthlink.net, Jun 2002.

ShotSpotter.com, "ShotSpotter," ShotSpotter, Inc., 2002, Available Online, [http://www.shotspotter.com/g-index.html/], ShotSpotter.com, Jul 2002.

Sivitz, Laura, "Airport to Test McLean Company's Iris Scanner," The Washington Post Company, 26 Jul 2001, [http://www.washtech.com/news/emerging/11450-1.html], washtech.com, Oct 2001.

Smith, Daniel, Col., USA, Retired, "The World at War," Center for Defense Information, 1 Jan 2001, Available Online, [http://www.cdi.org/dm/2001/issue1/world.html], CDI.org, 25 May 2002.

Soto, Carlos A., "Look Me in the Eye – or in the Face," Government Computer News, pp. 30-31, Vol. 21, No. 9, 29 Apr 2002.

Speir, Michelle, "The New Face of Security," Federal Computer Week, pp. 31-38, Vol. 16, No. 5, 4 Mar 2002.

Staedter, Tracy, "Face Recognition: A Camera and Algorithm Know It's You," Technology Review Magazine, pp. 86-87, Vol. 104, No. 9, Nov 2001.

Stikeman, Alexandra, "Recognizing the Enemy," Technology Review, Dec 2001, Available Online, [http://www.technologyreview.com/articles/stikeman1201.asp], TechnologyReview.com, May 2002.

Stikeman, Alexandra, "Recognizing the Enemy," Technology Review Magazine, pp. 48-49, Vol. 104, No. 10, Dec 2001.

Sullivan, Bob, "Big Brother Spending Spiked in 2001," MSNBC, 15 Apr 2002, Available Online, [http://www.msnbc.com/news/738958.asp/], MSNBC.com, Jun 2002.

Sullivan, Bob, "Identity Theft Easy for Terrorists," MSNBC, 27 Sep 2001, Available Online, [http://www.msnbc.com/news/634409.asp], MSNBC.com, Sep 2001.

Sullivan, Bob, "Warming to Big Brother," MSNBC, 14 Nov 2001, [http://www.msnbc.com/news/654959.asp], Nov 2001.

Sullivan, Brian, "Biometric Driver's Licenses within Five Years?" CNN, 3 May 2002, [http://www.cnn.com/2002/TECH/industry/05/03/biometric.licenses.idg/index.html], 15 May 2002.

Talbot, David, "Detecting Bioterrorism," Technology Review Magazine, pp. 34-37, Vol. 104/No. 10, Dec 2001.

Tarquinio, J. Alex, "10 Break-Throughs: How American Ingenuity Can Help Us Win," Reader's Digest, Feb 2002, pp. 73-78.

Tarquinio, J. Alex, "American Ingenuity Answers the Call," Reader's Digest, 2002, Available Online, [http://www.rd.com/common/nav/index.jhtml?articleId=9524970/, RD.com], Jun 2002.

Tenner, Edward, "The Shock of the Old," Technology Review Magazine, pp. 50-51, Vol. 104, No. 10, Dec 2001.

"The Global Course of Information Revolution: Political, Economic, and Social Consequences," Conference Proceedings, National Defense Research Institute; 2000.

"The Global Course of Information Revolution: Technological Trends," Conference Proceedings, National Defense Research Institute; 2000.

Thorsberg, Frank, "PC World Poll Highlights Privacy Concerns," CNN, 8 Oct 2001, [http://www.cnn.com/2001/TECH/industry/10/08/privacy.poll.idg/index.html], Dec 2001.

TROA Staff Writer, "Striking a Balance," The Retired Officer Magazine, pp. 34-38, Vol. LVIII, No. 3, Mar 2002.

Tyson, Jeff, "How Airport Security Works," Marshall Brian's How Stuff Works, Available Online, [http://www.howstuffworks.com/airport-security.htm/printable/], How StuffWorks.com, Jun 2002.

U.S. Congress, Office of Technology Assessment, "Electronic Surveillance in a Digital Age," OTA-BP-ITC-149, U.S. Government Printing Office, Jul 1995.

U.S. Department of State, "Patters of Global Terrorism 2001," United States Department of State, May 2002.

United Press International (UPI), "Homeland Security: Parts 1 through 5," Washington Politics & Policy Desk, 12 Feb 2002, Available Online, [http://www.upi.com/print.cfm?storyID=10022002-072930-1521/], UPI.com, Jun 2002.

University of Michigan Document Center, "Crime Statistics," 1 April 2002, Available Online, [http://www.lib.umich.edu/govdocs/frames/statsfr.html], May 2002.

USCNS, "Road Map for National Security: Imperative for Change," U.S. Commission on National Security/21st Century, 15 Feb 2001, Available Online, [http://www.nssg.gov], 30 May 2002.

USDOT, "U.S. International Air Passenger and Air Freight Statistics," Office of the Assistant Secretary for Aviation and International Affairs, Available Online, [http://ostpxweb.dot.gov/aviation], U.S. Department of Transportation, Mar 2001.

Vasishtha, Preeti, "FAA Will Run Transportation Smart-Card Pilot," Government Computer News, 17 Jun 2002, p. 9.

Vasishtha, Preeti, "FinCEN Seeks Terrorists' Money Links," Government Computer News, 17 Jun 2002, p. 20.

Visionics Corporation, "Breaking News and Company Announcements," Visionics Corporation, Available Online, [http://ir.shareholder.com/vsnx/releases.cfm/], Shareholder.com, Jun 2002.

Wakefield, Jane, "Surveillance Cameras to Predict Behaviour," 1 May 2002, Available Online, [http://news.bbc.co.uk/hi/english/sci/tech/newsid_1953000/1953770.stm], BBC News, 10 May 2002.

Wakefield, Jane, “Watching Your Every Move,” 7 Feb 2002, Available Online, [http://news.bbc.co.uk/hi/english/sci/tech/newsid_1789000/1789157.stm], BBC News, 10 May 2002.

Wald, Matthew L., “U.S. Considers Requiring Cameras Providing Cabin Views,” The New York Times, 30 May 2002, Available Online, [http://www.nytimes.com/2002/05/31/national/31SECU.html], NYTimes.com, Jun 2002.

Waldrop, Mitchell M., “Grid Computing,” MIT Technology Review Magazine, pp. 30-37, Vol. 105, No. 4, May 2002.

Walsh Trudy, “GAO Urges Coordination of Homeland Security,” Government Computer News, p. 14, Vol. 21, No. 9, 29 Apr 2002.

Walsh, Trudy, “Will Health Databases Spot Bioterror Attacks?” Government Computer News, 18 Feb 2002, pp. 1, 16, and 17.

Watching the Watchers #1, “Your Papers, Please: From the State Drivers License to a National Identification System,” Electronic Privacy Information Center, Feb 2002, Available Online, [http://www.epic.org/privacy/id_cards/yourpapersplease.pdf], Mar 2002.

Watching the Watchers #2, “Paying For Big Brother: A Review of the Proposed FY2003 Budget for the Department of Justice,” Electronic Privacy Information Center, Feb 2002, Available Online, [http://www.epic.org/reports/paying_for_bb.pdf], Mar 2002.

Whitehouse, “Executive Order Establishing Office of Homeland Security,” Whitehouse News Release, 8 Oct 2001, Available Online, [http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html], 28 Feb 2002.

Whitehouse, “The Department of Homeland Security,” Whitehouse PDF Document, Jun 2002, Available Online, [http://www.whitehouse.gov/deptofhomeland/], 8 Jun 2002.

Whitehouse, “The President's Homeland Security Policy and Budget Priorities,” The Office of Homeland Security, 2002, Available Online, [http://www.whitehouse.gov/homeland], 7 Apr 2002.

Wilson III, Sam B., “Micro Air Vehicles,” DARPA, 30 Jun 1998, Available Online, [http://www.darpa.mil/tto/programs/mavg.html], DARPA.mil, Jul 2002.

Wilson, Jim, “Homeland Security: We Have the Technology to Stop Terrorists Dead in Their Tracks,” Popular Science, Jan 2002, pp. 50-55.

Woodward, John D., Jr., “Use Biometrics to Protect America,” RAND Review, Dec 2001, Available Online, [http://www.rand.org/publications/randreview/issues/rr.12.01/], RAND.org, Jun 2002.

World Future Society, “Special Report – Trends and Forecasts for the Next 25 Years,” 2002, Available Online, [http://www.wfs.org], WFS.org, 19 May 2002.

World Global Trends, “Extracts from Major Reports and Key Findings,” 2002, Available Online, [http://www.t21.ca], 16 May 2002.

Xerox Palo Alto Research Center (PARC), 2001, [http://www.parc.xerox.com/parc-go.html], ubiq.com, Sep 2001.

Xerox Palo Alto Research Center (PARC), 2001, [http://www.ubiq.com/hypertext/weiser/UbiHome.html], ubiq.com, Apr 2002.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alex Bordersky, Information Systems Technology, Code IS
   Naval Postgraduate School
   Monterey, California

4. Dale Courtney, Information Systems Technology, Code IS
   Naval Postgraduate School
   Monterey, California

5. Dan C. Boger, Information Systems Department, Code IS
   Naval Postgraduate School
   Monterey, California

6. John Arquilla, Code C41
   Naval Postgraduate School
   Monterey, California

7. Frank Barrett, Graduate School of Business and Public Policy, Code SM
   Naval Postgraduate School
   Monterey, California

8. Theodore Lewis, Computer Science Department, Code CS
   Naval Postgraduate School
   Monterey, California

9. Nancy Roberts, Graduate School of Business and Public Policy, Code SM
   Postgraduate School
   Monterey, California

10. Captain Nicolas Yamodis, MC, USN
    Naval Medical Information Management Center
    Bethesda, Maryland

11. Lieutenant Commander Richard E. Makarski, MSC, USN
    Naval Postgraduate School
    Monterey, California

12. Lieutenant Jose A. Marrero, USNR
Naval Postgraduate School
Monterey, California